EXHIBIT H

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

MOBILE EQUITY CORP.,	§	
	§	
***Plaintiff*,**	§	
	§	
v.	§	**Civil Action No. 2:21-cv-126**
	§	
WALMART INC.,	§	
	§	**JURY TRIAL**
Defendant	§	
	§	

ORIGINAL COMPLAINT

Plaintiff Mobile Equity Corp. ("MEC") files this Original Complaint against Defendants Walmart Inc. ("Walmart" or "Defendant"), alleging as follows:

I. INTRODUCTION

1. MEC invented a novel and cost-effective technical structure for conducting mobile-payment transactions, making them more secure, convenient, and efficient. It filed a provisional patent for this ground-breaking invention in 2009—years before Apple Pay, Samsung Pay, and Walmart Pay were released.[1]

2. MEC sought patent protection on its intellectual property, raised venture capital to build its business and platform, developed a working mobile-payments platform it demoed, and obtained its first patent in November 2013. MEC approached the industry to revolutionize its systems with its patented technology, but, after years of hard work, MEC's innovations were simply taken without its permission.

[1] Apple Pay was released in October 2014. Samsung Pay was released in August 2015. Walmart Pay was released in December 2015.

3. In 2015, Walmart was considering multiple mobile-payment solutions. Walmart was demoing a mobile-payments solution created by the Merchant Customer Exchange ("MCX"), a large consortium of major U.S. retailers (*e.g.*, Walmart, Target, 7 Eleven, and CVS), which it had helped found years before. By the summer of 2015, MCX had been delayed multiple times, had proven difficult to implement, and looked unlikely to succeed.[2]

4. By, at least the fall of 2015, Walmart had changed course from MCX. Instead, it chose to incorporate MEC's patented technology into a new solution it called Walmart Pay. Walmart first launched Walmart Pay in December 2015 (over two years after MEC's first patent issued).

5. Walmart Pay is a Walmart service that provides a mobile-payment technology that allows a Walmart customer, using a Walmart-provided app, to "use your phone to pay quickly, easily, & touch-free at checkout."[3] Walmart Pay incorporates MEC's patented technology, without MEC's permission. It infringes MEC's Patents.

6. MEC's technology has been successful for Walmart. Walmart has repeatedly praised the solution Walmart Pay represents. Walmart Pay processes billions of dollars annually for Walmart. But Walmart has not compensated MEC for the use of MEC's invention.

7. MEC's business has suffered because of Walmart's infringement. This action is to remedy that infringement and to require Walmart to respect MEC's patent rights.

---

[2] *See, e.g.*, https://digital.hbs.edu/platform-rctom/submission/mcx-and-currentc-how-to-become-the-laughingstock-of-the-mobile-payments-industry/ .

[3] *See, e.g.*, https://www.walmart.com/cp/walmart-pay/3205993. Walmart Pay is discussed in detail later in this Complaint. Walmart Pay, as accused of infringement in this case, includes the uses of Walmart Pay in connection with any form of payment that uses the Walmart Pay process, including but not limited to "Scan & Go" and any other uses of Walmart Pay.

II. NATURE OF THE SUIT

8. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

III. THE PARTIES

9. Plaintiff **Mobile Equity Corp.** is a Delaware corporation with a principal place of business in the Plano, Texas area within this District.

10. Defendant **Walmart Inc.** is a Delaware corporation with a principal place of business at 702 S.W. 8th Street #555, Bentonville, Arkansas 72716. Walmart Inc. may be served through its registered agent in Texas, CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

IV. JURISDICTION AND VENUE

11. As an action under the patent laws of the United States, this Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

12. This Court has personal jurisdiction over Defendant Walmart.

13. Walmart has committed, and continues to commit, acts of infringement in this District, has conducted business in this District, and/or has engaged in continuous and systematic activities in this District.

14. This Court has personal jurisdiction over Walmart in this action because Walmart has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Walmart would not offend traditional notions of fair play and substantial justice. Walmart has committed and continues to commit acts of infringement in this District by, among other things, using, offering to sell, and selling products and/or services that infringe the Asserted Patents, including Walmart Pay.

15. This Court has specific personal jurisdiction over Walmart in this action pursuant to due process and the Texas Long-Arm Statute because the claims asserted herein arise out of or are related to Walmart's voluntary contacts with this forum, such voluntary contacts including but not limited to: (i) at least a portion of the actions complained of herein; (ii) purposefully and voluntarily placing Walmart Pay into this District and into the stream of commerce with the intention and expectation that it will be acquired by customers and used in this District; or (iii) regularly doing or soliciting business, engaging in other persistent courses of conduct, or deriving substantial revenue from goods and services, including Walmart Pay, provided to customers in Texas and in this District.

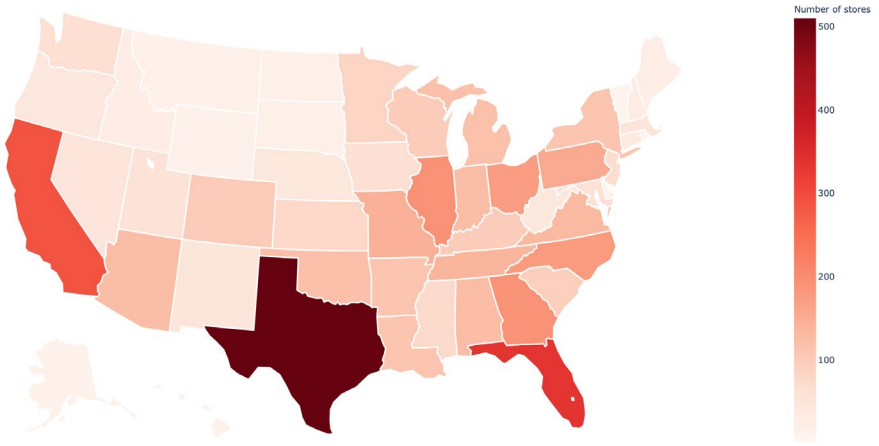
16. Venue is proper in this Court under 28 U.S.C. §§ 1391(b)(3) and 1400(b) for at least the reasons set forth above. Walmart is registered to do business in Texas, and Walmart has transacted business in this District. Walmart has regular and established places of business in this District. Walmart has committed acts of direct and indirect infringement in this District.

17. Walmart offers its products and/or services, including those accused herein of infringement, to customers and potential customers located in Texas and in this District. As non-limiting examples, Walmart distributes products directly to customers and through its partners, including through Apple's App Store and Google's Google Play. Among its other businesses, Walmart is in the business of providing mobile-payment services in this District.

A. Walmart Has an Extensive Presence in Texas and in This District

18. Walmart operates over 500 Walmart stores in Texas. Walmart operates more stores in Texas than it does in any other state, approximately 50% more stores than its next largest state (Florida).[4] The following 2020 image shows the distribution of Walmart stores by state:

[4] *See, e.g.,* Walmart Inc. 2021 10-K Annual Report, at 26. (available at https://stock.walmart.com/investors/financial-information/sec-filings/default.aspx).



19. Walmart's stores include multiple stores within this District, including locations in, at least, the following cities in this District: Anna; Athens; Atlanta; Beaumont; Bonham; Bridge City; Carthage; Center; Crockett; Cross Roads; Denison; Denton; Flower Mound; Frisco; Gainesville; Gilmer; Gun Barrel; Henderson; Hickory Creek; Highland Village; Jacksonville; Jasper; Kilgore; Liberty; Lewisville; Livingston; Longview; Lufkin; Lumberton; Marshall; McKinney; Mineola; Mt. Pleasant; Nacogdoches; New Boston; Palestine; Plano; Port Arthur; Princeton; Prosper; Roanoke; Sherman; Silsbee; Sulphur Springs; Texarkana; Tyler; West Orange; Woodville; and Vidor. A Walmart store has been present in Marshall since, at least, 1986.

20. Walmart operates, at least, nineteen distribution centers in Texas. Those include distribution centers within this District, including locations in, at least, the following cities in this District: Fort Worth (in Denton County); Palestine; Sanger; and Terrell.

21. Walmart operates a number of corporate offices in Texas. Those include, at least, technology development centers, including one in this District in Plano, Texas.

22. Walmart employs over 150,000 people in Texas, has collected $1.8 billion in taxes in Texas, and has paid over $500 million in taxes and fees in its fiscal year ending in 2020.[5]

[5] *See, e.g.*, https://corporate.walmart.com/our-story/locations/united-states/texas#.

B. Walmart Pay was Tested and Used in Texas and in This District

23. Walmart Pay was tested in select Walmart stores starting in December 2015.[6] Walmart Pay was tested in Texas and Arkansas stores before it was made available nationwide.[7]

24. Walmart Pay has been available nationwide since at least July 2016.[8]

25. Walmart Pay has been used in this District for many years. Walmart Pay has been put into service in this District, including by Walmart and its customers. Walmart has distributed the Walmart Pay application is this District, including distributing the Walmart Pay application through third-parties such as Apple and Google.

26. Walmart Pay is used in this District to, at least, receive an identifier to initiate a transaction that identifies a Walmart terminal (*e.g.*, a point-of-sale terminal, a self-checkout terminal), such as an identifier exemplified in the Quick Response ("QR") code displayed on Walmart terminals in this District. Walmart Pay is used in this District to, at least, send a request for transaction information to a Walmart terminal in this District associated with the identifier. Walmart Pay is used in this District to, at least, receive transaction information from the Walmart terminal, including the amount of the transaction. Walmart Pay is used in this District to, at least, identify a purchase accounts and initiate a transaction.

27. Walmart derives financial benefits through its business in Texas and in this District.

28. On information and belief, Walmart Pay has been used in more Texas Walmart stores than those of any other individual state. On information and belief, more Walmart Pay transactions have occurred in Texas than in any other state.

---

[6] *See, e.g.*, https://corporate.walmart.com/newsroom/2015/12/10/walmart-introduces-walmart-pay

[7] *See, e.g.*, https://www.paymentssource.com/news/walmart-pay-launches-in-texas-arkansas; https://www.businesswire.com/news/home/20160516005840/en/Walmart-Introduces-Walmart-Pay-in-Texas.

[8] *See, e.g.*, https://corporate.walmart.com/newsroom/2016/07/06/walmart-pay-now-available-in-all-walmart-stores-nationwide.

V. BACKGROUND

A. MEC and the Patented Technology

1. The Financial Services Industry is an Active Area of Innovation

29. The financial-services industry is one of active change and innovation.

30. Finance and technological development have been linked throughout history. For example, writing in early civilization may have developed to record payments and debts. The term "fintech" has been coined to refer to the large number of technology companies that seek to revolutionize the financial industry.

31. The last 75 years have seen a great number of financial-services innovations that have fundamentally changed our day-to-day lives, such as, credit cards; automatic teller machines (ATM); online banking; automatic bill payment; mobile wallets; automated clearing house transfers (ACH); electronic benefit transfer cards (EBT); and cryptocurrencies.

32. Innovations in the financial technology are patented by institutions from banks (*e.g.*, Bank of America, JPMorgan Chase) to traditional technology companies (*e.g.*, IBM, Apple, Google, Microsoft). These companies often tout the number of patents that they hold.

33. Walmart, for example, has many patents related to financial technology, including mobile device payment.[9]

34. Mobile payment is and has been an active area of invention. Many different approaches to mobile payments exist.

[9] These are four examples of Walmart's mobile-device payment: U.S. Patent Nos. 10,803,435 ("Method for self-checkout with a mobile device"); 10,679,219 ("Method and apparatus for automated shopper checkout using radio frequency identification technology"); 10,269,003 ("System and method for transaction payments using a mobile device"); and 9,514,455 ("Mobile device payment").

35. Promoting financial-services innovation has been a theme of, at least, the three most recent presidential administrations.[10]

2. The Asserted Patents

36. This cause of action asserts infringement of United States Patent Nos. 8,589,236 (the "'236 Patent") and 10,535,058 (the "'058 Patent") (collectively, the "Asserted Patents" or the "MEC Patents").

37. The U.S. Patent & Trademark Office ("Patent Office") rigorously scrutinizes applications for FinTech-related inventions, such as the inventions in MEC's Patents. That includes a strict examination to determine if the patent applications claim patent-eligible subject matter under 35 U.S.C. § 101. Allowance rates for FinTech-related inventions are low. The Patent Office's allowance of patents in the FinTech technology area thus reflects that the patents are valid and claim eligible subject matter.

38. A true and correct copy of the '236 Patent, entitled "Mobile Payment Station System and Method," with Mr. Marwan Afana as the named inventor, is attached hereto as Exhibit 1.

39. The '236 Patent duly and legally issued on November 19, 2013.

40. MEC is the current owner by assignment of all rights, title, and interest in and under the '236 Patent. MEC has standing to sue for infringement of the '236 Patent.

[10] *See, e.g.*, https://obamawhitehouse.archives.gov/blog/2016/06/10/future-finance-now; https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf; https://hill.house.gov/news/documentsingle.aspx?DocumentID=8090 ("Biden Administration Expected to Aid FinTech Innovation").

41. A true and correct copy of the '058 Patent, entitled "Mobile Payment Station System and Method," with Mr. Marwan Afana as the named inventor, is attached hereto as Exhibit 2.

42. The '058 Patent duly and legally issued on January 14, 2020.

43. MEC is the current owner by assignment of all rights, title, and interest in and under the '058 Patent. MEC has standing to sue for infringement of the '058 Patent.

3. The Development of MEC's Patented Inventions

44. The Asserted Patents result from the inventive work of Marwan Afana. Mr. Afana devoted the last 11 years of his life pursuing his mobile-payment invention and building a business based around his technology. Sadly and tragically, Mr. Afana unexpectedly passed away in November 2020.

45. Mr. Afana immigrated to the Dallas area from Saudi Arabia in the 1980s to study electrical engineering. He then spent over 20 years working with large telecommunications companies—such as AT&T, Ericsson, Lucent, and MCI—developing their projects (some on a global scale) for mobile networks, point-of-sale systems, mobile imaging, and billing systems.

46. The intersection of his life's experience led Mr. Afana to see a novel solution for mobile payments. Based on his belief in his invention, Mr. Afana left his secure and lucrative engineering career to build MEC.

47. Mr. Afana's novel solution, reflected in the Asserted Patents, provides a revolutionary, elegant, and counter-intuitive payment system that improves the security and convenience of conventional merchant point-of-sale systems while reusing existing hardware. The solution understands the function and problems of traditional point-of-sale systems and cleverly engineers a way to build a new system that incorporates elements of existing systems to make payment transactions more secure, efficient, and convenient.

48. Mr. Afana worked for years to commercialize his creation. He established a business in Texas and secured millions of dollars in investments. He assembled a global team and built a working mobile-payments platform at MEC. Mr. Afana traveled the country (and the world) to meet with potential partners. MEC also secured global patent rights for Mr. Afana's invention.

i) Conventional Payment Systems

49. Conventional payment-card transactions (*e.g.*, "swiping" a credit card at the point of sale) are familiar to most adults. These transactions bundle transaction information and the purchaser's information into a transmission from the payment terminal. In the conventional approach, transactions are initiated and flow in a "forward" path from the payment terminal to an authorization server containing both the purchase and payment information.

50. The conventional architecture is based on receiving the customer's account number at the point-of-sale terminal (*e.g.*, through a "swipe" or near-field communications, "NFC," transmission) and then having the terminal transmit that information to the banks through payment-clearing networks. MEC's provisional patent application depicts this conventional architecture as follows:[11]

51. These conventional architectures are technical systems that have technical problems, including security vulnerabilities. One category of security vulnerability they suffer

[11] U.S. Provisional App. No. 61/279,322, at 10.

from is exposing a customer's account information (*e.g.*, credit card information). These vulnerabilities are the result of the structure of conventional systems.

52. One security vulnerability is at the point-of-sale terminal itself. The conventional systems, as they existed in 2009, required the customer to provide account information at the terminal, either through swiping the physical card, tapping the card, or through an NFC-protocol transmission.

53. This engineering design exposes the customer's information, risking its compromise, such as through a credit-card skimmer.

54. Walmart customers have been victims of such skimming attacks.[12] The customers of many other retailers have also been the targets of such attacks.[13]

55. This engineering design also exposes the customers' information because it is stored in the terminal. This risks that the information may be compromised, such as through hacking into the point-of-sale terminal, such as with a malware attack, or the transmission between the terminal and the servers.[14]

56. Walmart's point-of-sale systems have been targeted by hackers.[15] Other retailers have also been the targets of such attacks.

57. These security problems are data-security problems that specifically arise as a result of the way the conventional merchant payment networks receive and process sensitive customer-account data.

---

[12] *See, e.g.*, https://krebsonsecurity.com/2016/05/skimmers-found-at-walmart-a-closer-look/ .
[13] *See, e.g.,* https://www.arklatexhomepage.com/news/crime/credit-card-skimmer-found-on-gas-pump-at-marshall-convenience-store/ (Marshall, TX); https://wjla.com/news/local/giant-food-credit-card-data-breach (Washington D.C.).
[14] *See, e.g.*, https://docs.broadcom.com/doc/attacks-on-point-of-sale-systems-en.
[15] *See, e.g.*, https://www.wired.com/2009/10/walmart-hack/ .

ii) **MEC's Patented Improvements**

58. The claims of the MEC Patents improve upon the technical structure of payment systems and offer a number of benefits, including compatibility with existing systems, such as by allowing for the reuse of existing point-of-sale hardware by changing its operation. The claims allow a customer to execute a transaction without sharing confidential information (*e.g.*, a credit card number) with the point-of-sale terminal. The claims achieve this through a specific solution that, in part, engineers a counterintuitive change to the conventional communications flow, rearranging it from a "forward" flow to a "backward" flow.

59. This approach, unlike the conventional approach, can begin with a mobile device transmitting a specific identifier to a server (different types are discussed). For example, a mobile device can begin a transaction by scanning a QR code displayed on a payment terminal. The mobile device can then send a request to make the transaction, including the scanned identifier (*e.g.*, data that identifies a point-of-sale terminal) to a server. The server then, for example, can query the point-of-sale terminal for the transaction information, such as an amount. The server is able to identify the specific customer's account (*e.g.*, based on the customer sending a request to initiate the transaction), and then clears the transaction using available account information.

60. The MEC Patents thus ensure that confidential information is not accessed by, routed through, or stored in the point-of-sale terminal. The only data exposed at the point-of-sale terminal is, essentially, information that can be publicly known (*e.g.*, the identity of the terminal/merchant and the amount to be paid). The customer's account information is not exposed at the terminal and is instead, for example, kept securely with the customer's account. This technological change improves the security of sensitive customer data, such as credit card information. This improvement has tangible benefits, such as by reducing fraud costs and improving customer privacy.

61. The innovation of the MEC Patents provides, among other benefits, security and convenience benefits beyond conventional payment architectures, including NFC-based systems (such as Apple Pay). In addition to the security benefits discussed above, the MEC Patents also provide additional benefits, some of which include:

a. First, the solution is compatible with most point-of-sale systems (through changing their programming) and mobile-devices and does not require a merchant to purchase new devices or complex technologies (*e.g.*, NFC or chip-readers). This reduces cost and complexity.

b. Second, the solution is compatible with most mobile devices. It does not require a mobile device with a new technology such as an NFC element. This increases the number of potential users and makes the technology more accessible.

c. Third, the approach allows transactions to execute electronically (*e.g.*, without a physical "swipe"). This makes all payments "contactless," which has several benefits, including speeding up the transaction process, which further reduces costs (*e.g.*, those related to waiting for checkout).

d. Fourth, unlike other mobile payment solutions, MEC's approach lets the merchant communicate the payment amount directly to the payment server. This eliminates payment-amount error (or fraud) that can result from allowing a payor (*e.g.*, the customer) to manually entering the amount.

62. In short, MEC created an elegant approach that simultaneously offers significant benefits and is, at the same time, compatible with and deployable on existing systems while improving the payment system infrastructure.

63. This approach was novel. And the patented MEC solution is not only different from the prior art, it is, essentially, the opposite of the prior art.

64. Initiating a transaction, at the point-of-sale, by transmitting a request to a server is contrary to conventional systems known in the art.

65. The Patent Office reaffirmed the unconventional nature of the MEC Patents' claims during their extensive prosecution, including during the six-plus-year examination of the '058 Patent. In that proceeding, MEC explained how its inventions improved the security of and ease

of use of conventional mobile-payment systems. Conventional systems "expose[d] payment credentials to the merchant's terminal," which can be "vulnerable at the merchant terminal to security threats."[16] The MEC Patents' claims, in contrast, "recit[e] a changed transaction process that modifies the messaging of these prior solutions. This improves on the technical problems of NFC and user-entered transaction information by modifying how the messaging for a transaction is performed."[17] The Patent Office allowed the claims, reaffirming that they claim patent-eligible subject matter.

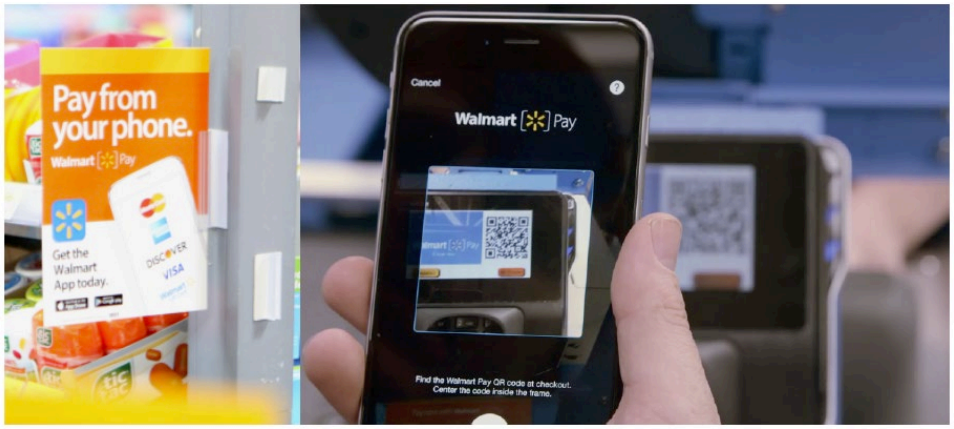
B. Walmart's Infringement

66. Walmart Pay uses Mr. Afana's invention without MEC's permission. It infringes the MEC Patents.

67. Walmart Pay is a mobile-payment solution that Walmart first introduced on December 10, 2015[18] and fully deployed—in over 4,600 stores—by July 6, 2016.[19] This was after two years after MEC's first patent issued and after MEC demonstrated its technology to the industry.

68. Walmart Pay allows Walmart customers to pay, at any Walmart register, using their mobile phone. The customer initiates payment by scanning the QR code presented at the payment terminal:

[16] U.S. Patent App. No. 14/082,425, July 19, 2019 Response to Final Rejection, at 7–12.
[17] U.S. Patent App. No. 14/082,425, July 19, 2019 Response to Final Rejection, at 7–12.
[18] https://corporate.walmart.com/newsroom/2015/12/10/walmart-introduces-walmart-pay.
[19] https://corporate.walmart.com/newsroom/2016/07/06/walmart-pay-now-available-in-all-walmart-stores-nationwide.



69. Generally, once the app is setup, all the user has to do is scan the QR code on a Walmart terminal to complete payment.[20] The mobile device uses the QR code to "send[] a signal to Walmart's server that it's okay to use Walmart Pay for that particular purchase."[21] The QR code "itself does not transmit any financial information."[22] To make Walmart Pay possible, Walmart installed proprietary software upgrades to its point-of-sale systems.[23]

70. When Walmart launched Walmart Pay it described it as "like no other mobile payments solution available today."[24] Walmart's senior vice president explained that "[t]he simplicity and ease of Walmart Pay comes not only from how it works, but also in how it's been built: We made a strategic decision to design Walmart Pay to work with almost any smartphone and accept almost any payment type – even allowing for the integration of other mobile wallets in

---

[20] https://corporate.walmart.com/newsroom/videos/b-roll-using-walmart-pay; *see also* https://www.youtube.com/watch?v=8BQrNNEJDag ("Walmart Introduces Walmart Pay"); https://www.youtube.com/watch?v=5Vrns65-M78 ("How to Register to use Walmart Pay").

[21] https://www.walmart.com/cp/walmart-pay/3205993.

[22] https://www.walmart.com/cp/walmart-pay/3205993.

[23] *See, e.g.*, https://www.cnbc.com/2015/12/09/wal-mart-launches-its-own-take-on-mobile-pay.html

[24] https://corporate.walmart.com/newsroom/2015/12/10/walmart-introduces-walmart-pay; *see also* https://www.youtube.com/watch?v=x0RL1M244VM; https://corporate.walmart.com/newsroom/2016/07/06/walmart-pay-now-available-in-all-walmart-stores-nationwide

the future. The result is an innovation that will make the ease of mobile payments a reality for millions of Americans."[25] Walmart has continued to provide, to promote, and use Walmart Pay from when it first launched in December 2015 to present.

71. Before Walmart's release of Walmart Pay in December 2015, Walmart had engaged in a trial of the CurrentC mobile-payment system produced by MCX. Walmart never deployed CurrentC beyond a Columbus, Ohio test.

72. CurrentC's development ran into significant problems, including technical problems.

73. Walmart ultimately did not use CurrentC. Nor did Walmart deploy Apple Pay.[26] Instead, Walmart adopted the technology of Walmart Pay—MEC's technology.

VI. CLAIMS

74. Walmart has been on notice of the Asserted Patents since, at least, the filings of this Complaint and on information and belief, as detailed above, has been on notice of the Asserted Patents prior to the filing of this Complaint.

75. Walmart has been on notice of its infringement since at least the filing of this Complaint and on information and belief, as detailed above, has been on notice of its infringement prior to the filing of this Complaint.

A. Infringement of the '236 Patent

76. The allegations of each foregoing paragraph are incorporated by reference as if fully set forth herein and form the basis for the following cause of action against Defendant.

77. Walmart Pay is covered by at least claim 1 of the '236 Patent.

---

[25] https://corporate.walmart.com/newsroom/2015/12/10/walmart-introduces-walmart-pay

[26] *See, e.g.*, https://www.washingtonpost.com/news/business/wp/2014/09/11/clash-of-the-titans-wal-mart-rejects-apple-pay-to-pursue-its-own-mobile-payment-system/.

78. Walmart has directly infringed and continues to infringe at least claim 1 of the '236 Patent in violation of 35 U.S.C. § 271(a) by, directly or through intermediaries and without MEC's authority, making, using, selling, and/or offering to sell Walmart Pay in the United States, or importing Walmart Pay into the United States.

79. Further and in the alternative, Walmart has been actively inducing infringement of at least claim 1 of the '236 Patent in violation of 35 U.S.C. § 271(b). Users of Walmart Pay directly infringed at least claim 1 of the '236 Patent when they used Walmart Pay in the ordinary, customary, and intended way. Defendant's inducements included, without limitation and with specific intent to encourage the infringement, knowingly inducing consumers to use Walmart Pay within the United States in the ordinary, customary, and intended way by, directly or through intermediaries, supplying Walmart Pay to consumers within the United States and instructing and encouraging such consumers (for example, via distributing Walmart Pay to mobile phones through app stores and instructing users to use Walmart Pay) how to use Walmart Pay in the ordinary, customary, and intended way, which Defendant knows or should know infringes at least claim 1 of the '236 Patent. Defendant's inducements may further include, without limitation and with specific intent to encourage the infringement, knowingly inducing customers to use Walmart Pay within the United States, or knowingly inducing customers to use Walmart Pay within the United States, by, directly or through intermediaries, instructing and encouraging such customers to make, use, sell, or offer to sell Walmart Pay in the United States, which Defendant knows or should know infringes at least claim 1 of the '236 Patent.

80. Further and in the alternative, Defendant has been actively contributing to infringement of at least claim 1 of the '236 Patent in violation of 35 U.S.C. § 271(c). Defendant has installed the Walmart Pay system and application to process payments wherein a mobile device

scans a QR code presented at the point-of-sale terminal, which is especially made or especially adapted to practice the invention claimed in at least claim 1 of the '236 Patent. Each Walmart Pay component constitutes a material part of the claimed invention recited in at least claim 1 of the '236 Patent and not a staple article or commodity of commerce because it is specifically configured according to at least claim 1 of the '236 Patent. Defendant's contributions include, without limitation, making, offering to sell, and/or selling within the United States, and/or importing into the United States, Walmart Pay, which include one or more components, knowing each component to be especially made or especially adapted for use in an infringement of at least claim 1 of the '236 Patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use.

81. Further and in the alternative, Walmart has infringed and continues to infringe at least claim 1 of the '236 Patent in violation of 35 U.S.C. § 271(f) via providing Walmart Pay to locations outside of the United States, such as Canada.

82. Walmart knew or should have known of the '236 Patent but was willfully blind to the existence of the '236 Patent. Walmart has had actual knowledge of the '236 Patent since at least as early as the filing and service of this Complaint. By the time of the trial of this case, Walmart will have known and intended that its continued actions since receiving such notice would infringe and actively induce and contribute to the infringement of one or more claims of the '236 Patent. Walmart's infringement of the '236 Patent has been willful and deliberate.

83. Walmart and/or users (*e.g.*, Walmart's customers) use Walmart Pay to conduct a transaction between a merchant (Walmart) and/or terminal (Walmart's point-of-sale terminal) and a customer (an individual Walmart customer), where the customer uses a mobile device (*e.g.*, a mobile phone such as a smartphone).

84. Walmart Pay is available for Android and iOS-based mobile devices.

85. Walmart Pay allows a customer to "[p]ay with any iOS or Android smartphone[.]"[27]

86. Walmart Pay "works with any iOS or Android device."[28]

87. Walmart receives a merchant identifier from the mobile device operated by the customer (*e.g.*, a Walmart Pay user), the merchant identifier indicating a request to initiate a transaction with a merchant terminal identified by the merchant identifier, wherein the merchant identifier does not indicate a transaction amount for the transaction.

88. On information and belief, for example, Walmart receives a merchant identifier from the mobile device operated by the customer, for example, data reflected in a QR code.

89. Walmart Pay's scan of the QR code "sends a signal to Walmart's server that it is okay to use Walmart Pay for that particular purchase" and the "signal itself," containing data reflected in the QR code, "does not transmit any financial information":

> We keep our technology simple, & we use tested hardware that's already in place. Walmart Pay doesn't use near-field communication (NFC). Instead, our customers use their smartphones to scan a secure QR code displayed on the same PIN pads at checkout that are being used now. A customer's scan sends a signal to Walmart's server that it is okay to use Walmart Pay for that particular purchase. The signal itself does not transmit any financial information.[29]

90. For example, Walmart discloses the following usage of Walmart Pay through displaying and scanning a QR code:[30]

---

[27] https://corporate.walmart.com/newsroom/2015/12/10/walmart-introduces-walmart-pay.
[28] https://corporate.walmart.com/newsroom/2015/12/10/walmart-introduces-walmart-pay.
[29] https://www.walmart.com/cp/walmart-pay/3205993.
[30] https://corporate.walmart.com/_download?id=00000155-c082-de62-a7fd-e6eefa980000.

91. Walmart shows an example use of this same QR code, in which the transaction amount in the example is $36.26.[31]

92. Decoded, this QR code provides the following data: WMT00041080065392146065O612F2AC609CC4D10144.

93. That data does not include a transaction amount.

94. That data does not include any payment information (*e.g.*, credit card information).

95. Walmart receives transaction information from the merchant terminal in response to the transaction information request, the transaction information including the transaction amount for the transaction.

96. For example, Walmart receives transaction information for a point-of-sale terminal, including the transaction amount (*e.g.*, the total amount due for the transaction).

97. Walmart Pay's scan of the QR code "sends a signal to Walmart's server that it is okay to use Walmart Pay for that particular purchase":

[31] https://corporate.walmart.com/newsroom/videos/b-roll-using-walmart-pay (at 32s).

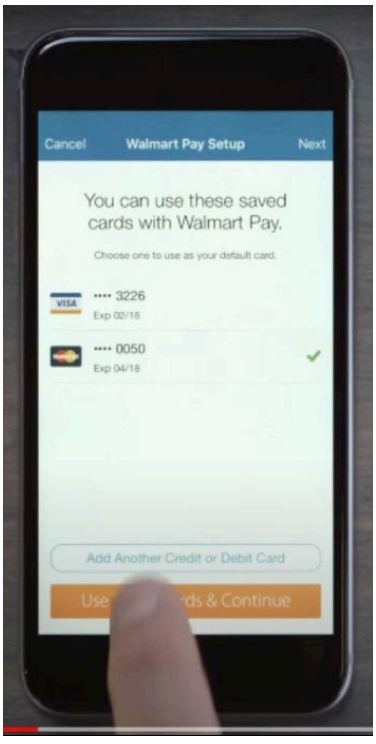
> We keep our technology simple, & we use tested hardware that's already in place. Walmart Pay doesn't use near-field communication (NFC). Instead, our customers use their smartphones to scan a secure QR code displayed on the same PIN pads at checkout that are being used now. A customer's scan sends a signal to Walmart's server that it is okay to use Walmart Pay for that particular purchase. The signal itself does not transmit any financial information.[32]

98. The signal received by Walmart's server includes, on information and belief, the identity of the Walmart store and/or point-of-sale terminal.

99. The Walmart server, on information and belief, receives the amount of the transaction from the point-of-sale terminal and/or the mobile device.

100. Walmart identifies a purchase account associated with the customer and a deposit account associated with the merchant.

101. For example, Walmart identifies a purchase account associated with an individual customer (*e.g.*, a credit card, debit card, or other stored-value card saved using Walmart Pay):[33]



[32] https://www.walmart.com/cp/walmart-pay/3205993.
[33] https://corporate.walmart.com/newsroom/videos/how-to-register-to-use-walmart-pay.

102. Walmart identifies a deposit account associated with the merchant in order to complete the transaction, displaying, for example, that "Payment approved" on the point-of-sale terminal.[34]

103. Walmart initiates the transaction between the merchant and the customer for the transaction amount received from the merchant terminal and the identified purchase account associated with the customer and the identified deposit account associated with the merchant.

104. Walmart initiates the transaction between the merchant (*e.g.*, Walmart or the individual Walmart point-of-sale terminal) and the customer, for the transaction amount received from the merchant terminal (*e.g.*, the purchase amount) and the identified purchase account (*e.g.*, the credit card or other stored-value card) associated with the customer and the identified deposit account associated with the merchant.

105. Walmart and/or users of Walmart's infringing instrumentalities (*e.g.*, Walmart's customers) use the Walmart Pay application to conduct a transaction between a terminal (Walmart's point-of-sale terminal) and a customer (an individual Walmart customer), where the customer uses a mobile device (*e.g.*, a mobile phone).

B. Infringement of the '058 Patent

106. The allegations of each foregoing paragraph are incorporated by reference as if fully set forth herein and form the basis for the following cause of action against Defendant.

107. Walmart Pay is covered by at least claim 1 of the '058 Patent.

108. Walmart has directly infringed and continues to infringe at least claim 1 of the '058 Patent in violation of 35 U.S.C. § 271(a) by, directly or through intermediaries and without MEC's

[34] https://corporate.walmart.com/newsroom/videos/how-to-register-to-use-walmart-pay.

authority, making, using, selling, or offering to sell Walmart Pay in the United States, or importing Walmart Pay into the United States.

109. Further and in the alternative, Walmart has been actively inducing infringement of at least claim 1 of the '058 Patent in violation of 35 U.S.C. § 271(b). Users of Walmart Pay directly infringed at least claim 1 of the '058 Patent when they used Walmart Pay in the ordinary, customary, and intended way. Defendant's inducements included, without limitation and with specific intent to encourage the infringement, knowingly inducing consumers to use Walmart Pay within the United States in the ordinary, customary, and intended way by, directly or through intermediaries, supplying Walmart Pay to consumers within the United States and instructing and encouraging such consumers (for example, via distributing Walmart Pay to mobile phones through app stores and instructing users to use Walmart Pay) how to use Walmart Pay in the ordinary, customary, and intended way, which Defendant knows or should know infringes at least claim 1 of the '058 Patent. Defendant's inducements may further include, without limitation and with specific intent to encourage the infringement, knowingly inducing customers to use Walmart Pay within the United States, or knowingly inducing customers to use Walmart Pay within the United States, by, directly or through intermediaries, instructing and encouraging such customers to make, use, sell, or offer to sell Walmart Pay in the United States, which Defendant knows or should know infringes at least claim 1 of the '058 Patent.

110. Further and in the alternative, Walmart has been actively contributing to infringement of at least claim 1 of the '058 Patent in violation of 35 U.S.C. § 271(c). Defendant has installed the Walmart Pay system and application to process payments wherein a mobile device scans a QR code presented at the point-of-sale terminal, which is especially made or especially adapted to practice the invention claimed in at least claim 1 of the '058 Patent. Each Walmart Pay

component constitutes a material part of the claimed invention recited in at least claim 1 of the '058 Patent and not a staple article or commodity of commerce because it is specifically configured according to at least claim 1 of the '058 Patent. Defendant's contributions include, without limitation, making, offering to sell, and/or selling within the United States, and/or importing into the United States, Walmart Pay, which includes one or more components, knowing each component to be especially made or especially adapted for use in an infringement of at least claim 1 of the '058 Patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use.

111. Further and in the alternative, Walmart has infringed and continues to infringe at least claim 1 of the '058 Patent in violation of 35 U.S.C. § 271(f) via providing Walmart Pay to locations outside of the United States, such as Canada.

112. Walmart knew or should have known of the '058 Patent but was willfully blind to the existence of the '058 Patent. Walmart has had actual knowledge of the '058 Patent since at least as early as the filing and service of this Complaint. By the time of the trial of this case, Defendant will have known and intended that its continued actions since receiving such notice would infringe and actively induce and contribute to the infringement of one or more claims of the '058 Patent. Defendant's infringement of the '058 Patent has been willful and deliberate.

113. Walmart and/or users (*e.g.*, Walmart's customers) use Walmart Pay to conduct a transaction between a merchant (*e.g.*, Walmart) and/or terminal (*e.g.*, Walmart's point-of-sale terminal) and a customer (*e.g.*, an individual Walmart customer), where the customer uses a mobile device (*e.g.*, a mobile phone such as a smartphone).

114. Walmart receives, at its payment processing server, a terminal identifier from the mobile device operated by the customer (*e.g.*, a Walmart Pay user), the terminal identifier

indicating a request to initiate a transaction with a terminal identified by the terminal identifier, wherein the terminal identifier does not indicate a transaction amount for the transaction.

115. For example, Walmart receives a terminal identifier from the mobile device operated by the customer, for example, data reflected in a QR code.

116. The terminal identifier (*e.g.*, data evidenced in a QR code) indicates a request to initiate a transaction with a terminal (*e.g.*, the point-of-sale terminal) identified by the terminal identifier.

117. Walmart's payment processing server sends, in response to receiving the terminal identifier, a transaction information request to the terminal associated with the terminal identifier.

118. For example, Walmart sends, in response to receiving the identifier (*e.g.*, "customer scan" containing a "secure QR code") from the mobile device operated by the customer, a transaction information request (from "Walmart's server") to the particular point-of-sale terminal associated with the "customer scan" and QR code, as further detailed above in connection with Walmart's scanning and processing QR code data.

119. Walmart receives, at its payment processing server, transaction information from its terminal in response to the transaction information request, the transaction information including the transaction amount for the transaction.

120. For example, Walmart receives transaction information for a point-of-sale terminal, including the transaction amount (*e.g.*, the total amount due for the transaction).

121. The signal received by Walmart's server includes, on information and belief, the identity of the Walmart store and/or point-of-sale terminal.

122. The Walmart server, on information and belief, receives the amount of the transaction from the point-of-sale terminal and/or the mobile device.

123. Walmart identifies, at its payment processing server, a customer account associated with the customer and a terminal account associated with the terminal.

124. For example, Walmart identifies a purchase account associated with an individual customer (*e.g.*, a credit card, debit card, or other stored-value card saved using the customer's Walmart Pay application).[35]

125. Walmart identifies a deposit account associated with the merchant in order to complete the transaction, displaying, for example, that "Payment approved" on the point-of-sale terminal.[36]

126. Walmart initiates the transaction between the merchant and the customer for the transaction amount received from the merchant terminal and the identified purchase account associated with the customer and the identified deposit account associated with the merchant.

127. Walmart initiates the transaction between the merchant (*e.g.*, Walmart or the individual Walmart point-of-sale terminal) and the customer, for the transaction amount received from the merchant terminal (*e.g.*, the total purchase amount) and the identified purchase account (*e.g.*, the credit card or other stored-value card) associated with the customer and the identified deposit account associated with the merchant, as shown below.

128. Walmart, at its payment processing server, initiates the transaction between the terminal and the customer for the transaction amount received from the terminal.

129. Walmart initiates the transaction between the terminal (*e.g.*, the individual Walmart point-of-sale terminal) and the customer, for the transaction amount received from the terminal

[35] https://corporate.walmart.com/newsroom/videos/how-to-register-to-use-walmart-pay.
[36] https://corporate.walmart.com/newsroom/videos/how-to-register-to-use-walmart-pay.

(*e.g.*, the total purchase amount) and the identified customer account (*e.g.*, the customer's credit card or other stored-value card).

VII. JURY DEMAND

130. Pursuant to Federal Rule of Civil Procedure 38(b), MEC requests a jury trial of all issues triable of right by a jury.

VIII. PRAYER FOR RELIEF

MEC respectfully requests the Court enter an order providing the following relief:

1. A judgment in favor of MEC that Defendant has infringed each Asserted Patent, whether literally or under the doctrine of equivalents;

2. A judgment that such infringement of each Asserted Patent has been willful and deliberate as described herein;

3. A judgment and order permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Asserted Patents pursuant to 35 U.S.C. § 283;

4. A judgment and order requiring Defendant to pay MEC its damages, costs, expenses, and pre-judgment and post-judgment interest for Defendant's infringement of each Asserted Patent as provided under 35 U.S.C. § 284, including supplemental damages for any continuing post-verdict or post-judgment infringement with an accounting as needed;

5. A judgment and order requiring Defendant to pay MEC enhanced damages for willful infringement as provided under 35 U.S.C. § 284;

6. A judgment and order finding this case exceptional and requiring Defendant to pay MEC its reasonable attorneys' fees and costs incurred in this litigation pursuant to 35 U.S.C. § 285, together with pre-judgment and post-judgment interest thereon; and

7. Awarding MEC all such other and further relief, in law or equity, as the Court deems just and proper under the circumstances.

Dated: April 07, 2021

Respectfully submitted,

/s/ William E. Davis, III
William E. Davis, III
Texas State Bar No. 24047416
bdavis@davisfirm.com

Christian J. Hurt
Texas State Bar No. 24059987
churt@davisfirm.com

Rudolph "Rudy" Fink IV
Texas State Bar No. 24082997
rfink@davisfirm.com

THE DAVIS FIRM, P.C.
213 N. Fredonia Street, Suite 230
Longview, Texas 75601
Telephone: (903) 230-9090
Facsimile: (903) 230-9661

ATTORNEYS FOR PLAINTIFF MOBILE EQUITY CORP.

EXHIBIT 1

US008589236B2

(12) **United States Patent**
Afana

(10) **Patent No.: US 8,589,236 B2**
(45) **Date of Patent: Nov. 19, 2013**

(54) **MOBILE PAYMENT STATION SYSTEM AND METHOD**

(75) Inventor: **Marwan Monir Afana**, Allen, TX (US)

(73) Assignee: **Faber Financial, LLC**, Encinitas, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 84 days.

(21) Appl. No.: **12/906,989**

(22) Filed: **Oct. 18, 2010**

(65) **Prior Publication Data**

US 2011/0093351 A1 Apr. 21, 2011

Related U.S. Application Data

(60) Provisional application No. 61/279,322, filed on Oct. 19, 2009.

(51) **Int. Cl.**
G06Q 20/00 (2012.01)
G06Q 40/00 (2012.01)

(52) **U.S. Cl.**
USPC **705/16**; 705/39

(58) **Field of Classification Search**
USPC 705/16
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,868,391	B1	3/2005	Hultgren	
7,873,573	B2 *	1/2011	Realini	705/39
8,073,424	B2 *	12/2011	Sun et al.	455/406
2002/0181710	A1	12/2002	Adam et al.	
2007/0255652	A1 *	11/2007	Tumminaro et al.	705/39
2009/0248537	A1	10/2009	Sarkeshik	
2011/0041180	A1 *	2/2011	Jakobsson et al.	726/23

OTHER PUBLICATIONS

PCT International Search Report and Written Opinion, PCT Application No. PCT/US2010/053059, Dec. 23, 2010, 10 pages.

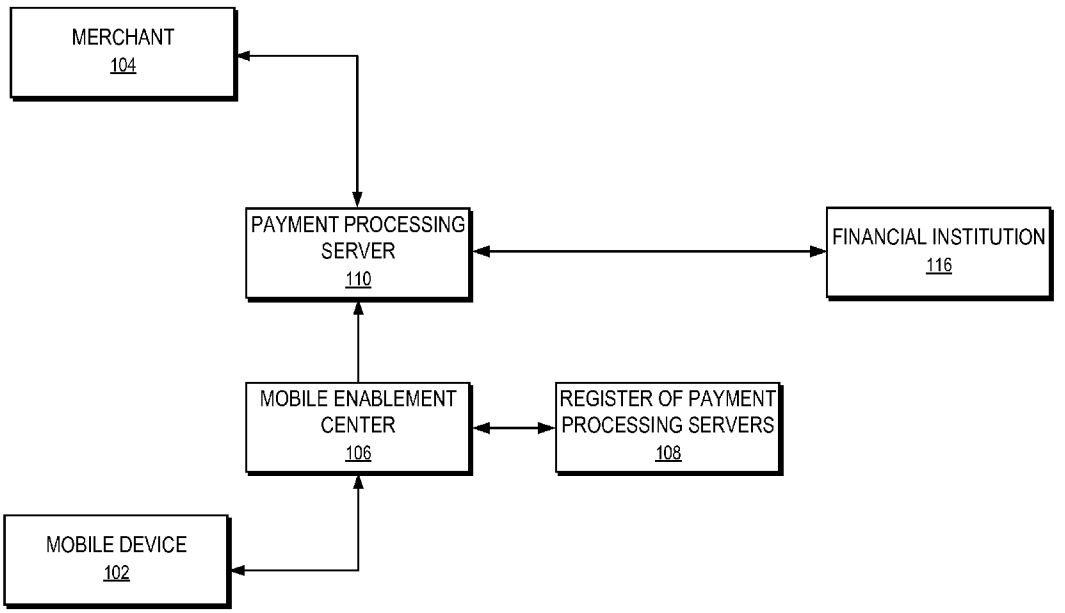
* cited by examiner

Primary Examiner — Garcia Ade
(74) *Attorney, Agent, or Firm* — Fenwick & West LLP

(57) **ABSTRACT**

A mobile device is used to initiate and execute a transaction between a customer and a merchant. A mobile device is used to initiate a point of sale transaction, wherein a merchant ID is sent to a payment processing server. Responsive to receiving a communication from the mobile device, the payment processing server requests transaction information from the merchant, wherein the merchant is identified based on the provided merchant ID. The merchant can provide transaction information such as the total sale amount to the payment processing server. The payment processing server can authenticate the customer and initiate a purchase transaction with the appropriate financial institutions associated with the customer and the merchant. The payment processing server can send a confirmation of the executed transaction to the merchant and the mobile device.

19 Claims, 11 Drawing Sheets



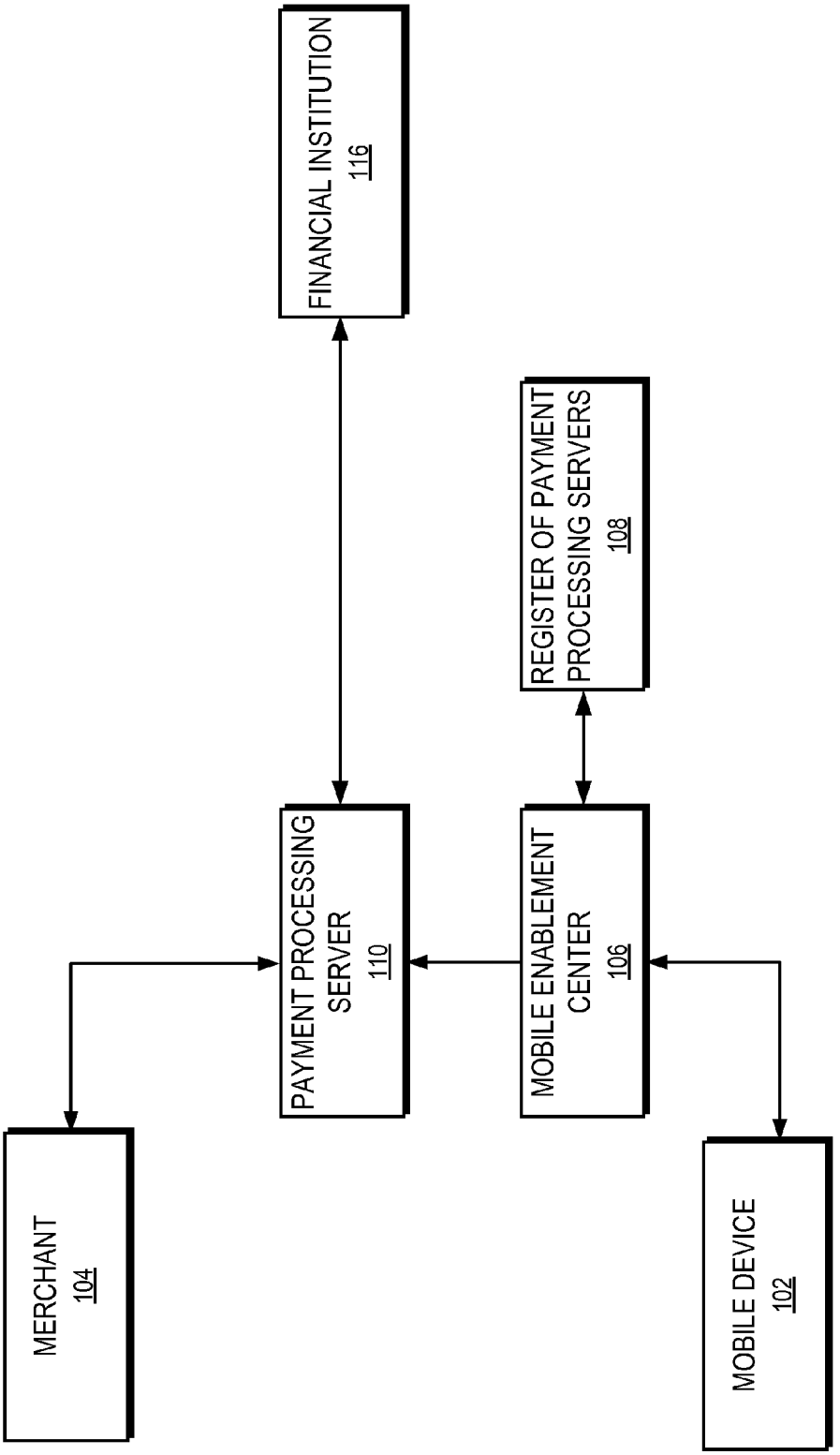

FINANCIAL INSTITUTION
116
REGISTER OF PAYMENT PROCESSING SERVERS
108
PAYMENT PROCESSING SERVER
110
MOBILE ENABLEMENT CENTER
106
MERCHANT
104
MOBILE DEVICE
102

FIG. 1

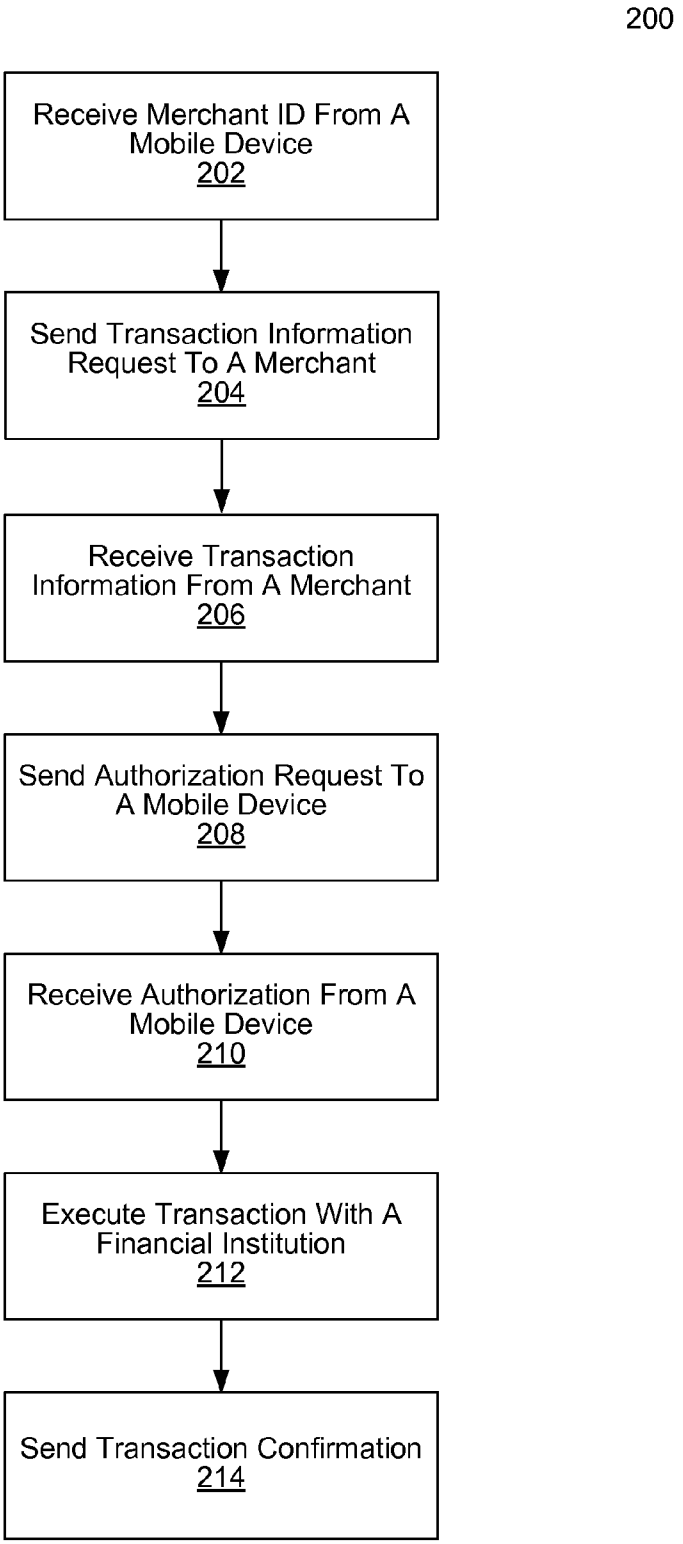

200
Receive Merchant ID From A Mobile Device
202
Send Transaction Information Request To A Merchant
204
Receive Transaction Information From A Merchant
206
Send Authorization Request To A Mobile Device
208
Receive Authorization From A Mobile Device
210
Execute Transaction With A Financial Institution
212
Send Transaction Confirmation
214

FIG. 2

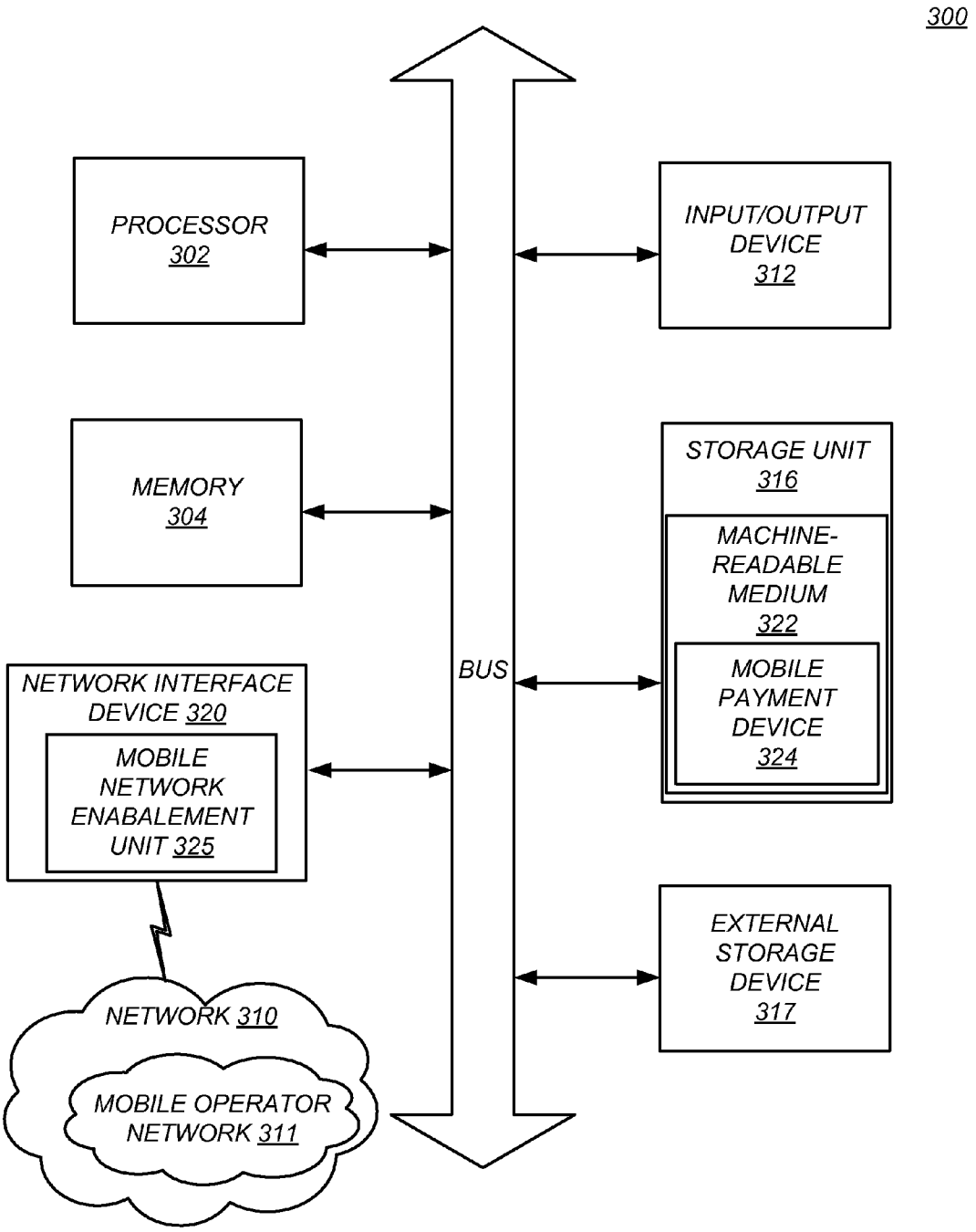

300
PROCESSOR 302
INPUT/OUTPUT DEVICE 312
MEMORY 304
STORAGE UNIT 316
MACHINE-READABLE MEDIUM 322
MOBILE PAYMENT DEVICE 324
BUS
NETWORK INTERFACE DEVICE 320
MOBILE NETWORK ENABALEMENT UNIT 325
EXTERNAL STORAGE DEVICE 317
NETWORK 310
MOBILE OPERATOR NETWORK 311

FIG. 3

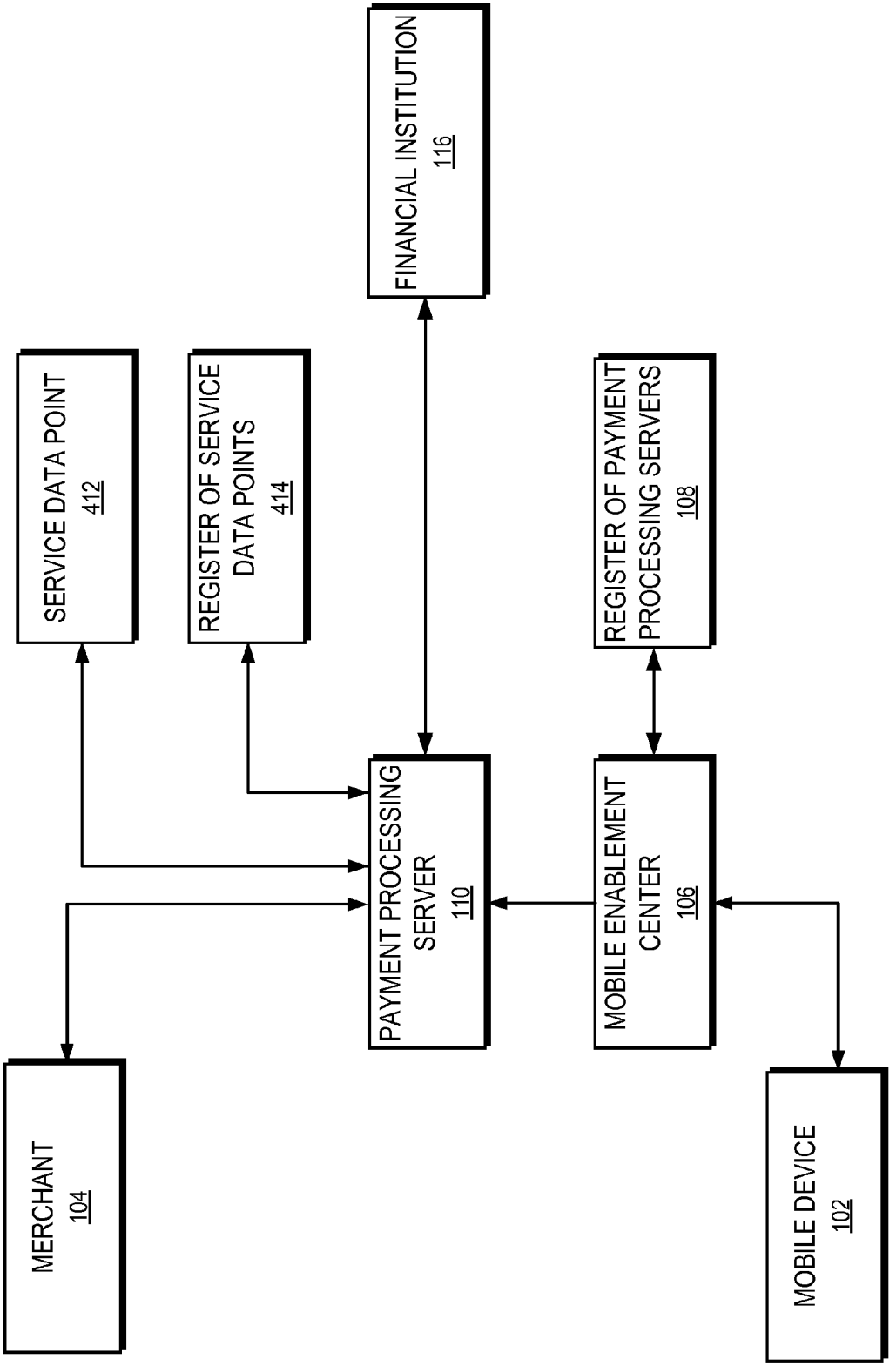

FINANCIAL INSTITUTION
116
SERVICE DATA POINT
412
REGISTER OF SERVICE DATA POINTS
414
REGISTER OF PAYMENT PROCESSING SERVERS
108
PAYMENT PROCESSING SERVER
110
MOBILE ENABLEMENT CENTER
106
MERCHANT
104
MOBILE DEVICE
102

FIG. 4

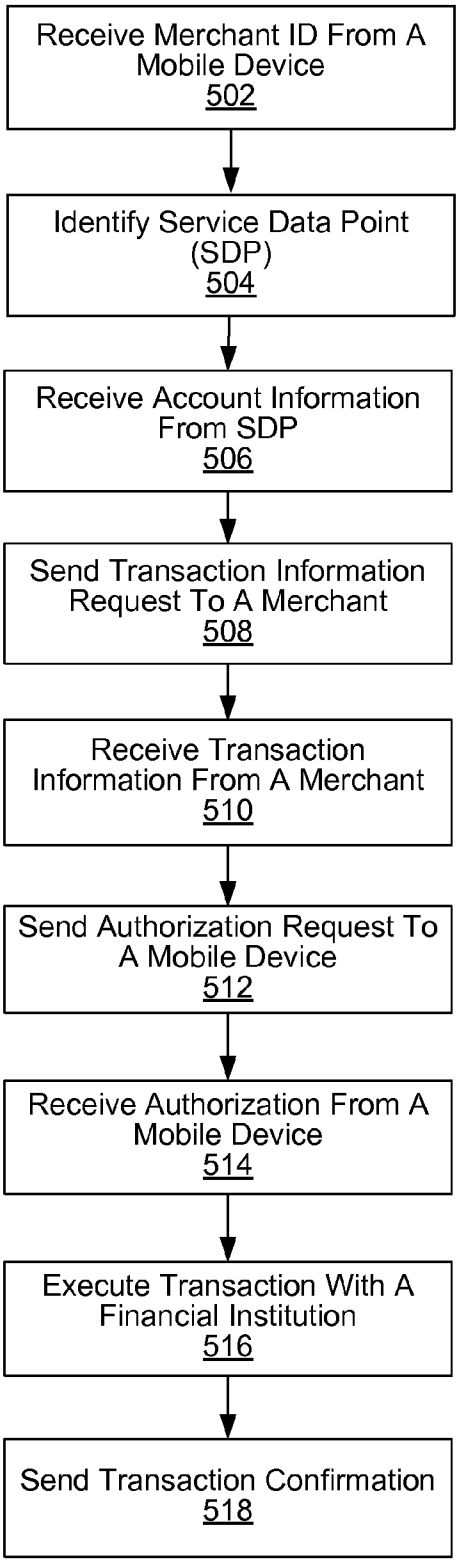

500
Receive Merchant ID From A Mobile Device
502
Identify Service Data Point (SDP)
504
Receive Account Information From SDP
506
Send Transaction Information Request To A Merchant
508
Receive Transaction Information From A Merchant
510
Send Authorization Request To A Mobile Device
512
Receive Authorization From A Mobile Device
514
Execute Transaction With A Financial Institution
516
Send Transaction Confirmation
518

FIG. 5

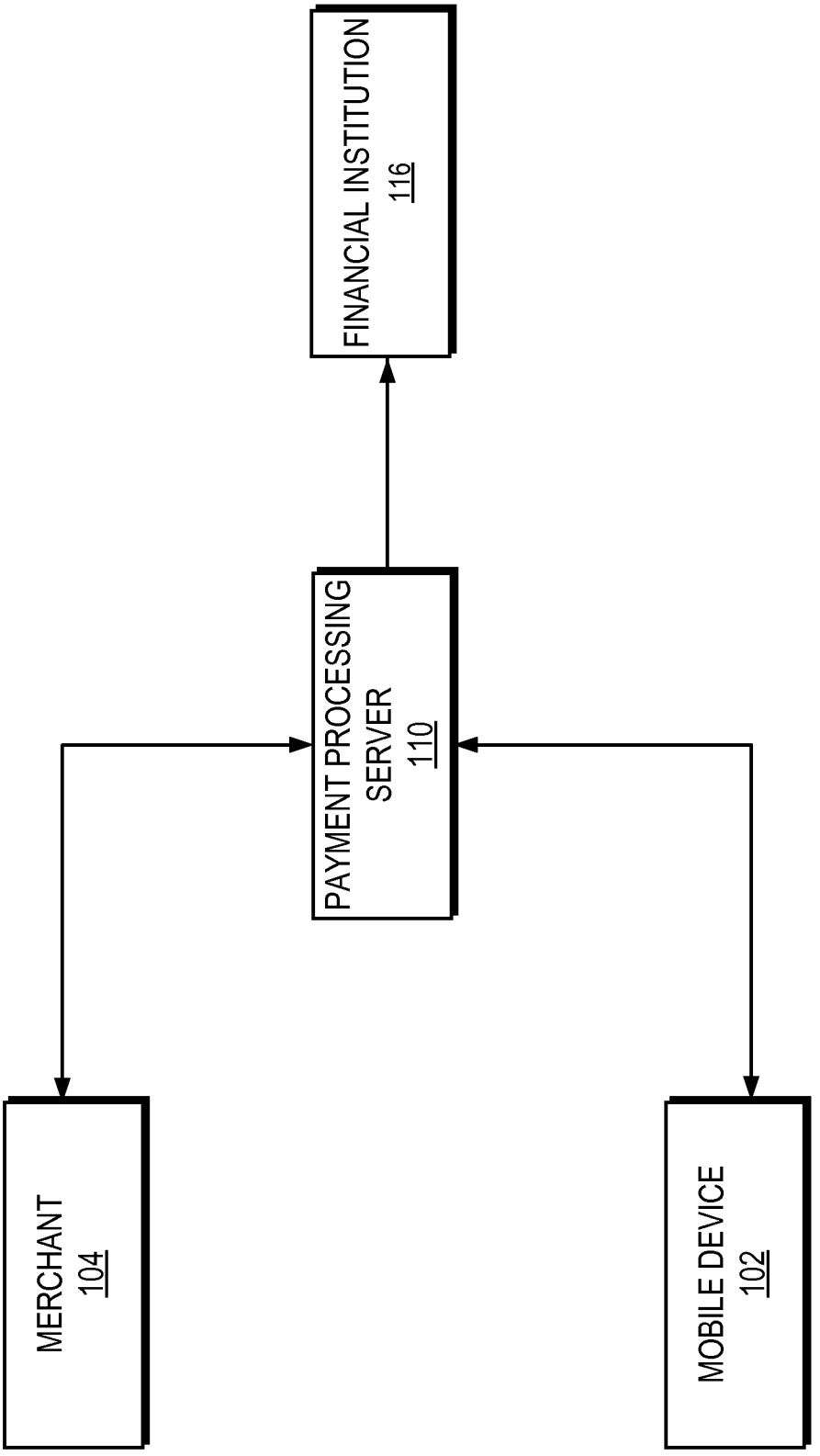

FINANCIAL INSTITUTION
116
PAYMENT PROCESSING SERVER
110
MERCHANT
104
MOBILE DEVICE
102

FIG. 6

700

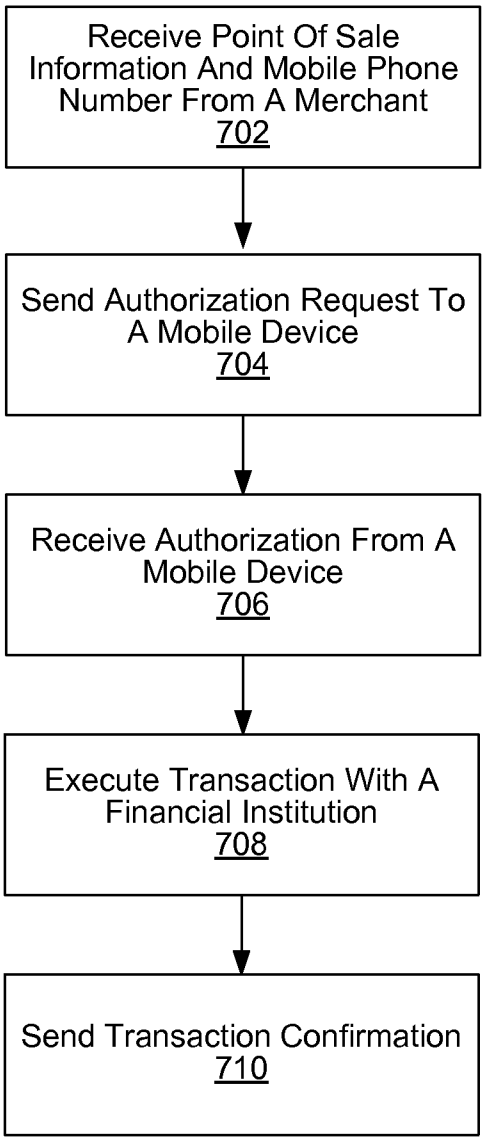

Receive Point Of Sale Information And Mobile Phone Number From A Merchant
702
Send Authorization Request To A Mobile Device
704
Receive Authorization From A Mobile Device
706
Execute Transaction With A Financial Institution
708
Send Transaction Confirmation
710

FIG. 7

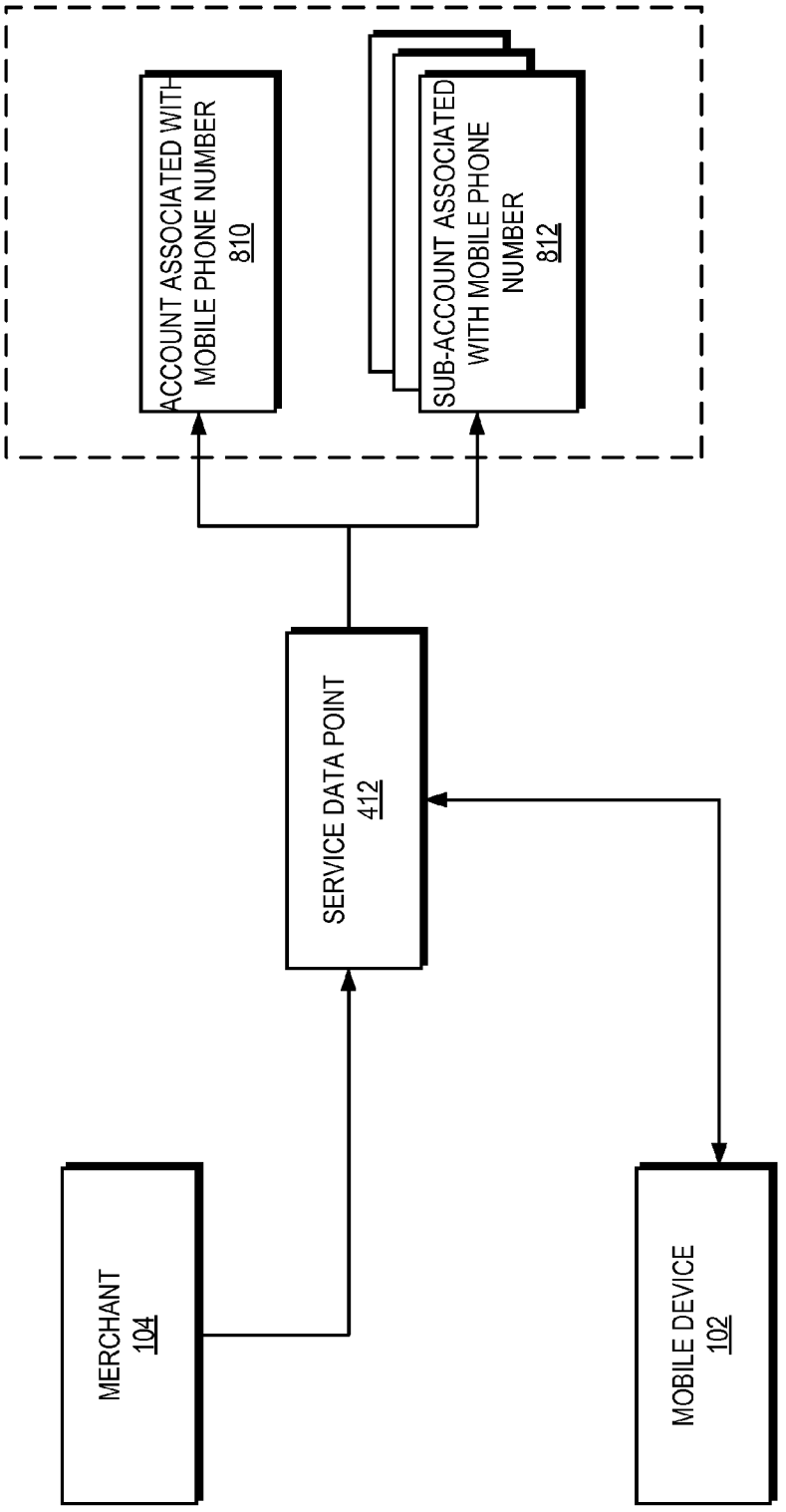

ACCOUNT ASSOCIATED WITH MOBILE PHONE NUMBER 810
SUB-ACCOUNT ASSOCIATED WITH MOBILE PHONE NUMBER 812
SERVICE DATA POINT 412
MERCHANT 104
MOBILE DEVICE 102

FIG. 8

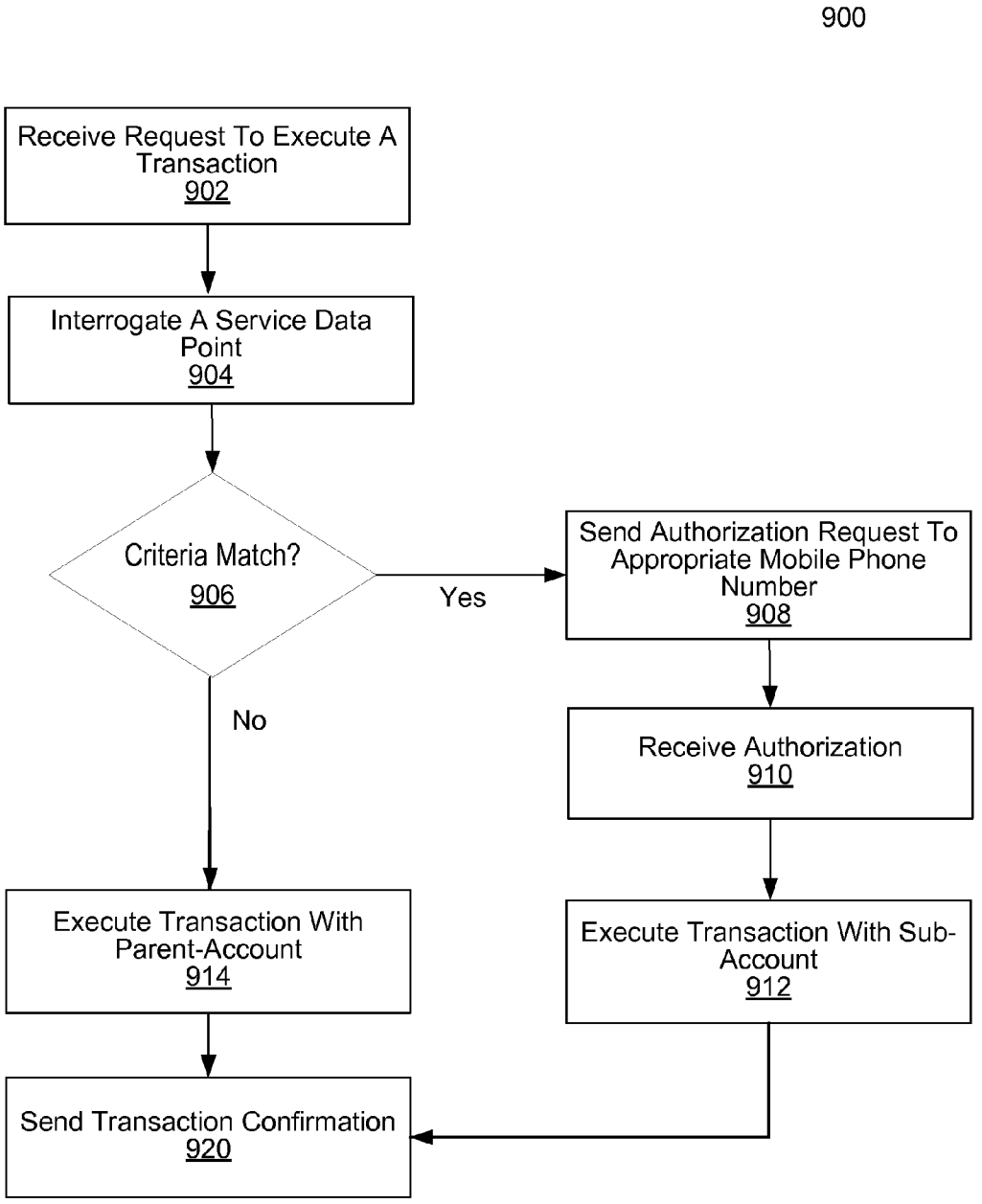

900
Receive Request To Execute A Transaction
902
Interrogate A Service Data Point
904
Criteria Match?
906
Yes
No
Send Authorization Request To Appropriate Mobile Phone Number
908
Receive Authorization
910
Execute Transaction With Sub-Account
912
Execute Transaction With Parent-Account
914
Send Transaction Confirmation
920

FIG. 9

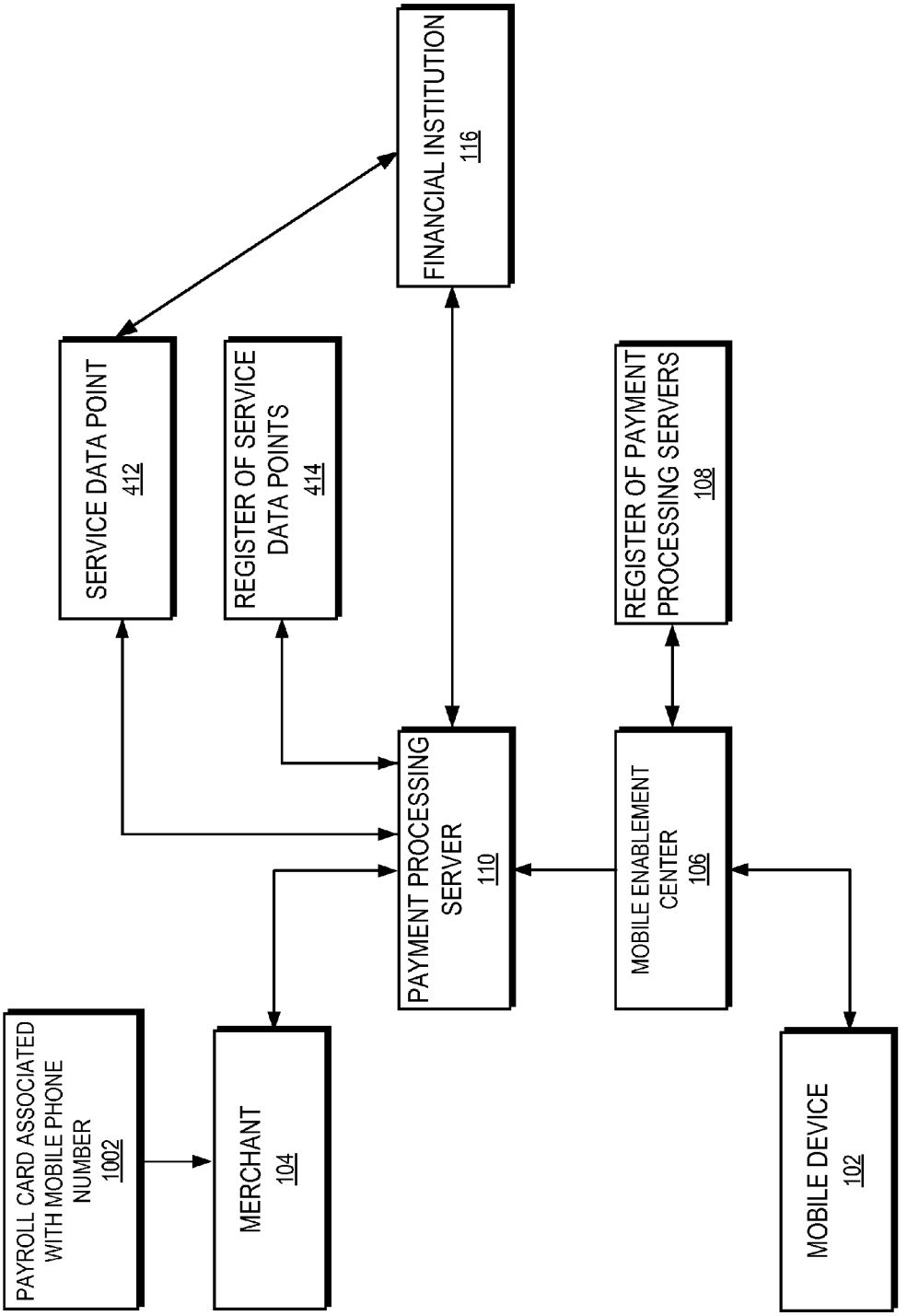

FINANCIAL INSTITUTION
116
SERVICE DATA POINT
412
REGISTER OF SERVICE DATA POINTS
414
REGISTER OF PAYMENT PROCESSING SERVERS
108
PAYMENT PROCESSING SERVER
110
MOBILE ENABLEMENT CENTER
106
PAYROLL CARD ASSOCIATED WITH MOBILE PHONE NUMBER
1002
MERCHANT
104
MOBILE DEVICE
102

FIG. 10

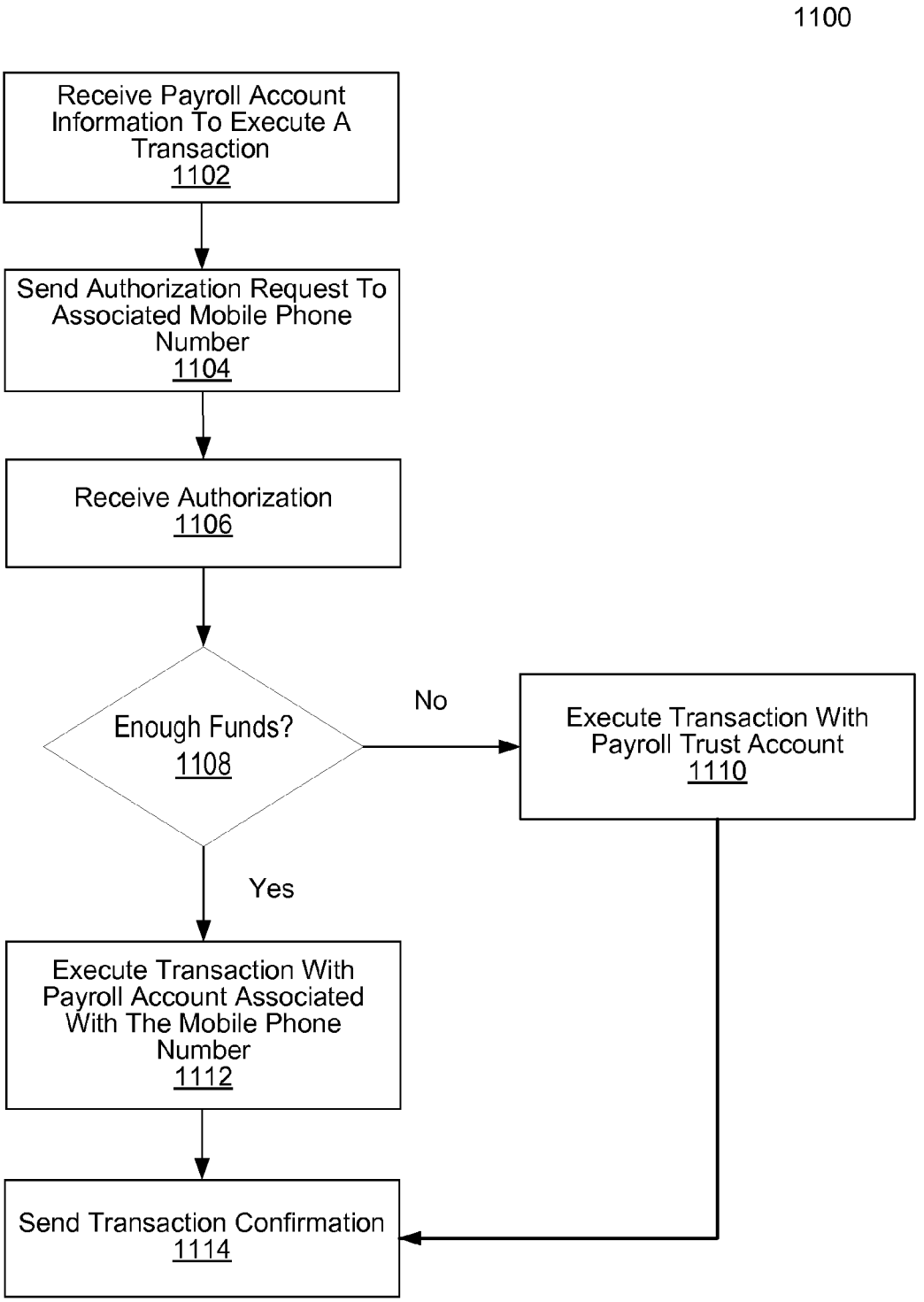

1100
Receive Payroll Account Information To Execute A Transaction
1102
Send Authorization Request To Associated Mobile Phone Number
1104
Receive Authorization
1106
Enough Funds?
1108
No
Execute Transaction With Payroll Trust Account
1110
Yes
Execute Transaction With Payroll Account Associated With The Mobile Phone Number
1112
Send Transaction Confirmation
1114

FIG. 11

MOBILE PAYMENT STATION SYSTEM AND METHOD

RELATED APPLICATIONS

This application claims priority from U.S. provisional application No. 61/279,322 filed on Oct. 19, 2009 which is incorporated by reference herein in its entirety.

FIELD OF THE INVENTION

This invention generally relates to the field of electronic commerce and more particularly to using mobile communication devices to execute a commercial transaction.

BACKGROUND OF THE INVENTION

Using a credit card, debit card, payroll card, senior benefit card, ATM card or any stored value card (hereafter credit card) and a point of sale terminal to purchase one or more items from a merchant has become commonplace. For example, in order to initiate a point of sale, a merchant can enter the total sale amount in a terminal. The merchant can receive a credit card from the customer to process the sale. Once the customer's credit card information is entered in a point of sale terminal, the information is sent to servers associated with a clearing house. The clearinghouse can authenticate the credit information and route the transaction based on the routing numbers associated with the credit card. The clearing house can execute a transaction with an appropriate financial institution and provide a confirmation of the executed transaction to the merchant's point of sale terminal. The merchant can print a confirmation of the executed transaction to receive a customer's approval.

Such a method of executing a transaction is beneficial because it is quick and reliable. Additionally, the customer can execute a purchase at any time regardless of whether the customer has cash on hand to purchase a product. However, such a method of executing transactions requires that the customer have a credit card. A customer can use the convenience of a card to execute transactions through a debit card if the customer has an associated debit account. However, many customers do not have bank accounts, and therefore do not have debit cards. Similarly, some customers, such as kids under a certain age may not have access to or qualify for a credit card but nevertheless may need a secure method of executing a transaction for purchase of goods.

Additionally, a customer using a credit card runs the risk of credit card fraud or fraudulent transactions. For example, if a customer's credit card is lost or stolen, another person who is not the owner of the card can execute a transaction with the card by simply presenting the card to a merchant. Since the merchant initiates the point of sale for each transaction, the clearing house and the financial institutions may not catch a fraudulent transaction unless reported by the owner of the credit card.

A customer may also not be able to use credit processing systems to execute a purchase if the customer does not have his or her card available at the merchant site. For example, a customer cannot borrow someone else's credit card to execute a transaction associated with his or her own account. Thus, credit cards or cards associated with financial institutions provide a less than optimal method for executing a transaction associated with a customer's credit or financial account.

A customer may also not be able to use credit processing systems to execute a purchase if the customer's card has a defective magnetic strip, chip or the electronic near field communication (NFC) apparatus on the card is defective. Additionally, a customer may be unable to use credit processing systems to execute a purchase if the point of sale terminal at the store is defective or has a defective NFC receiver that prevents it from reading card information.

SUMMARY OF THE INVENTION

It is a general object of the present invention to allow a customer to use a mobile communications device to initiate and execute a transaction by reversing the conventional direction of point of sale transaction initiation; that is the processing server opens communications towards point of sale terminal utilizing merchant ID or point of sale terminal ID, instead of the conventional method of point of sale terminal opening communications towards processing server.

It is a general object of the present invention to allow a customer to use a mobile communications device to initiate and execute a transaction, which overcomes the aforementioned problems with using a credit or debit card by taking advantage of the prevalence of mobile communications devices and the communications abilities of mobile devices.

It is also a general object of the present invention to allow a customer to use other methods such as calling an interactive voice response (IVR) system and using voice or dual-tone multi-frequency (DTMF) commands on a landline to initiate and execute a transaction, which overcomes the aforementioned problems with using a credit or debit card by taking advantage of the prevalence of telecommunication methods available today.

A mobile device can be used to initiate and execute a transaction with a merchant. A mobile device is used to initiate a point of sale transaction, wherein a merchant ID or, for example, a point of sale terminal ID (hereafter called "merchant ID") is sent to a payment processing server. Responsive to receiving a communication from the mobile device, the payment processing server requests transaction information from the merchant, wherein the merchant is identified based on the provided merchant ID. The merchant can provide transaction information such as the total sale amount to the payment processing server. The payment processing server can authenticate the customer and initiate a purchase transaction with the appropriate financial institutions associated with the customer and the merchant. The payment processing server can send a confirmation of the executed transaction to the merchant and the mobile device.

It is another general object of the present invention to use a point of sale terminal associated with a merchant to execute a transaction between a merchant and a customer. A merchant can provide point of sale information including the purchase amount, merchant ID and an account phone number associated with the customer. An account phone number can include a financial institution account number that belong to the customer, a phone number that is associated with a financial account number that belongs to the customer, a phone number that is used as an account number in a financial institution hereafter referred to as "account phone number.". Responsive to receiving point of sale information from the merchant, a payment processing server identifies an account associated with the account phone number and sends an authorization request to the account phone number. The customer can enter authorization personal identification information on a communications device and send it to the payment processing server. The payment processing server can authenticate the customer and initiate a purchase transaction with the appropriate financial institutions associated with the customer and

the merchant. The payment processing server can send a confirmation of the executed transaction to the merchant and the mobile device.

It is another general object of the present invention to use a payroll account associated with an account phone number to execute a transaction between a merchant and a customer. The point of sale transaction can be initiated by the merchant using the point of sale terminal or by a customer using a communications device or via an IVR call. A service data point (SDP) receives a merchant ID associated with the merchant and the account phone number associated with the customer and the payroll account. The payment processing server sends an authorization request to the account phone number. The customer can enter an authorization personal identification number on a mobile device associated with the account phone number and send it to the SDP. The SDP can authenticate the customer associated with the payroll account and initiate the purchase transaction between the merchant and the payroll account associated with the customer. The SDP can send a confirmation of the executed transaction to the merchant and the mobile device. The functionality of an SDP can be integrated in the mobile enablement center **106** and can be called either SDP or Mobile enablement center and vice versa. Similarly, the mobile enablement functionality center's functionality can be integrated in an SDP and be called the mobile enablement center or the SDP. For instance an implementation described below using an SDP can be carried out in a mobile enablement center and vice versa.

The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specification, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a high-level block diagram that illustrates a computing environment for using a mobile device to initiate a transaction according to one embodiment.

FIG. **2** is a flowchart illustrating a method of using a mobile device to initiate a transaction according to one embodiment.

FIG. **3** is a high-level block diagram illustrating a detailed view of a payment processing server for initiating a transaction using a mobile device according to one embodiment.

FIG. **4** is a high-level block diagram that illustrates a computing environment for using a mobile device to initiate a transaction according to one embodiment.

FIG. **5** is a flowchart illustrating a method of using a mobile device to execute a transaction according to one embodiment.

FIG. **6** is a high-level block diagram that illustrates a computing environment for using a mobile device to execute a transaction according to one embodiment.

FIG. **7** is a flowchart illustrating a method of using a mobile device to execute a transaction according to one embodiment.

FIG. **8** is a high-level block diagram that illustrates a computing environment for using a mobile device to execute a transaction associated with a sub-account according to one embodiment.

FIG. **9** is a flowchart illustrating a method of using a mobile device to execute a transaction associated with a sub-account according to one embodiment.

FIG. **10** is a high-level block diagram that illustrates a computing environment for using a payroll card to execute a transaction according to one embodiment.

FIG. **11** is a flowchart illustrating a method of using a payroll card to execute a transaction according to one embodiment.

The figures depict various embodiments of the present invention for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the invention described herein.

DETAILED DESCRIPTION OF THE INVENTION

A preferred embodiment of the present invention is now described with reference to the figures where like reference numbers indicate identical or functionally similar elements. Also in the figures, the left most digit(s) of each reference number corresponds to the figure in which the reference number is first used.

Reference in the specification to "one embodiment" or to "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiments is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" or "an embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

Some portions of the detailed description that follows are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps (instructions) leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, electromagnetic, radio or optical signals capable of being stored, transferred, combined, compared and otherwise manipulated. It is convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. Furthermore, it is also convenient at times, to refer to certain arrangements of steps requiring physical manipulations or transformation of physical quantities or representations of physical quantities as modules or code devices, without loss of generality.

However, all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or "determining" or the like, refer to the action and processes of a computer system, or similar electronic computing device (such as a specific computing machine), that manipulates and transforms data represented as physical (electronic) quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Certain aspects of the present invention include process steps and instructions described herein in the form of an algorithm. It should be noted that the process steps and instructions of the present invention could be embodied in software, firmware or hardware, and when embodied in software, could be downloaded to reside on and be operated from different platforms used by a variety of operating systems.

The invention can also be in a computer program product which can be executed on a computing system.

The present invention also relates to an apparatus for performing the operations herein. This apparatus may be specially constructed for the purposes, e.g., a specific computer, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a non-transitory computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, application specific integrated circuits (ASICs), or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus. Memory can include any of the above and/or other devices that can store information/data/programs. Furthermore, the computers referred to in the specification may include a single processor or may be architectures employing multiple processor designs for increased computing capability.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems may also be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the method steps. The structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the present invention as described herein, and any references below to specific languages are provided for disclosure of enablement and best mode of the present invention.

In addition, the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the present invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the claims.

FIG. **1** is a high-level block diagram that illustrates a computing environment for using a mobile device to initiate a transaction according to one embodiment. The computing environment may include a mobile device **102**, a mobile enablement center **106**, a register of payment processing servers **108**, a payment processing server **110**, a merchant **104** and a financial institution **116**.

FIG. **2** is a flowchart illustrating a method of using a mobile device to initiate a transaction according to one embodiment. For the purposes of discussion below, FIGS. **1** and **2** are discussed concurrently.

In one embodiment, the mobile device **102** initiates a point of sale transaction. A mobile device **102** can include any computing device having a processor and capability to communicate with others over a network or a communications link. Examples of a mobile device **102** include a cellular phone, personal device assistant (PDA), smart phone, laptop computer, desktop computer or other devices. The mobile device sends a merchant ID associated with a merchant to the payment processing server **106**. The merchant ID number is a unique identifier associated with a merchant. The merchant ID can include any information to identify or communicate with the associated number. For example, a merchant ID can include a point-of-sale terminal ID to be used by the merchant to execute the transaction. In other embodiments, the merchant ID can include an e-mail address or a phone number associated with the merchant.

In one embodiment, the customer can enter the merchant ID on to the mobile device **102** using the mobile device's input system, such as a keyboard or a touchpad etc. In other embodiments, the merchant ID information can be received by a camera on the mobile device **102**. In other embodiments, the merchant ID information can be displayed in plain view for customer to use. In other embodiments, the merchant ID information can be displayed in alphanumeric or bar code format for customer to use. In other embodiments, the merchant ID information can be received by the mobile device **102** through a communications link such as BLUETOOTH communications or RFID communications fields. For example, a merchant can have a point-of-sale terminal which broadcasts the merchant ID to mobile devices via a BLUETOOTH, laser, radio, infrared or close range electromagnetic field communications link. In one embodiment, the mobile device **102** sends the received merchant ID to another party over a communications network.

The mobile device **102** can use any available communications (COMM) method to send the merchant ID to the mobile enablement center **106**. It can use unstructured supplementary service data (USSD), short message service (SMS), multi-media message service (MMS), IVR, email, short message peer-to-peer (SMPP), Internet browser, an application executing on a mobile device, widget executing on a computing device, hard button (key), soft button (key) or any communication method available in the art in various wired or wireless technologies such as but not limited to code division multiple access (CDMA), wideband code divisional multiple access (WCDMA), integrated digital enhanced network (iDEN), Global System for Mobile Communications (GSM), one or more generations of wireless telephone technology, such as 2G, 3G, 4G, or any future generations of wireless telephone technology, Bluetooth, WiFi, worldwide interoperability for microwave access (WiMAX), Radio (short wave or other), infrared or any other communication method or protocol known in the art. Such a communication or other examples of communication are referred to herein, among other names, as COMM.

The mobile device **102** can use any available communications method (COMM) to send the merchant ID to the mobile enablement center **106**. In one embodiment, the mobile device **102** can send the merchant ID in an SMS message over a mobile communications network, such as GSM, iDEN or CDMA networks in any setup that could be 2G, 3G, 4G or any future evolution of wireless technology. In other instances, the mobile device can send multi-media messages (MMS). For example, the customer can take a picture of a barcode or a number identifier associated with the merchant ID and send the picture over a communications network. In another instance an application executing on the mobile device **102** can interpret or recognize the barcode or number identifier associated with the merchant ID to send over a communications network. In other embodiments, the communications network used by the mobile device **102** depends on the network capabilities of the mobile device **102**. For example, the mobile device can connect to a WiFi Network and send the merchant ID via email to the payment processing server **106** over the network. In one embodiment, the customer can enter the merchant ID via IVR from a landline telephone. In other embodiments, the customer can use a user interface associated with an application executing on the mobile device **102** to send the merchant ID to the mobile enablement center **106** over a communications network. The network used to con-

nect the mobile device **102**, the merchant **104**, the mobile enablement center **106**, the payment processing server **110**, the service data point **112** and the financial institution **116** is described in greater detail below.

In one embodiment, the merchant ID is sent to an appropriate payment processing server **110**. For example, a customer can provide a pre-set preference, wherein all transactions executed with the mobile device **102** are associated with a particular financial institution and routed through a particular payment processing server **110**. In an embodiment IPV6 protocols can be used to route the communications request to an appropriate payment processing server **110**. In another embodiment, the mobile device **102** sends the merchant ID to a mobile enablement center **106** over a communications network to be routed to an appropriate payment processing server **110**.

The mobile enablement center **106** is a platform that routes outgoing messages from the mobile devices **102** to the appropriate payment processing server **110**. The mobile enablement center **106** can receive routing requests from several service broadcast operators, such as mobile phone network operators, including GSM or CDMA network operators, landline phone operators, LAN operators, etc. For example, when mobile devices **102**, including landline or VOIP phones send an outgoing message, the service broadcast operator associated with the device or the phone number receives the outgoing message request. The service broadcast operator routes the outgoing message to the broadcast operator associated with the intended recipient of the message. In an embodiment of the invention, the mobile enablement center **106** receives a routing request from the service broadcast operator associated with the mobile device **102** or directly from the mobile device **102**. In one embodiment, the mobile enablement center **106** routes the message to an appropriate payment processing server **106** based on the outgoing message's phone number, the intended recipient's phone number, the merchant ID included in the message or any other data associated with the phone number. For example, if a user's phone number is associated with a particular financial institution **116**, the mobile enablement center **106** routes the message to a payment processing server **110** associated with the financial institution **116**.

In one embodiment, the payment processing server **110** interrogates a registry of payment processing servers **108** to identify an appropriate payment processing server **110**. For example a registry of payment processing servers **108** can include a listing of payment processing servers **110** based on the routing numbers or other identification information associated with each financial institution or based on coordinated new routing mechanism that may be mandated, devised or supervised by, for example, a standardization body, governmental body or consortium body of companies or leaders in the field.

A payment processing server **110** is a platform that executes a transaction between a customer, a financial institution **116** associated with the customer and a merchant **104**. Examples of a payment processing servers **110** include databases maintained by Visa, MasterCard, American Express, etc. In one embodiment, the payment processing server **110** receives **202** the merchant ID from the mobile device **102**. In another embodiment, the payment processing server **110** receives **202** the merchant ID in a message routed by the mobile enablement center **106**.

In one embodiment, the payment processing server **110** sends **204** a request for transaction information to the merchant **104** associated with the received merchant ID. Any communications method (COMM) known in the art can be used to communicate with the merchant **104**. For example, the payment processing center can send an SMS message, an e-mail message etc to a phone number or an email address associated with the merchant **104**. In one embodiment, the merchant ID can be associated with a merchant's unique point-of-sale terminal. In such an instance, the payment processing server **110** can send a communication to the point the particular point-of-sale terminal.

The merchant **104** can provide transaction information to send to the payment processing server **110**. Transaction information can include the total purchase price for the items the customer wants to purchase, an account number associated with the merchant, the mobile phone number provided by the customer etc. The merchant **104** can use any communications method (COMM) known in art to provide the transaction information to the payment processing server **110**. In one embodiment, the merchant can enter the total purchase amount on a point-of-sale terminal's keypad. A point of sale terminal can include a station wherein the merchant can swipe or key-in a customer's credit card or debit card to execute a purchase transaction. In another embodiment, the point of sale terminal can include a computing device, such as a machine to machine (M2M) device, mobile phone, a laptop or desktop computer, a tablet etc. In other embodiments, point of sale terminals can include established transaction terminals, such as an ATM or vending machine etc. In an instance where existing transaction terminals such as ATM or card-swipe terminals are used, the terminals can be updated via a firmware update to enable them to receive transaction information requests from a payment processing server **110**.

The payment processing server **110** receives **206** transaction information from the merchant **104**. In one embodiment, transaction information includes a phone number associated with the customer mobile device **102**. The payment processing server **110** authenticates the phone number associated with the mobile device **102**. In one embodiment, the payment processing server **110** authenticates the incoming message's phone number against the service broadcast operator network. For example, if a mobile phone number is associated with the T-MOBILE, the payment processing server **110** can query the T-MOBILE operator network **311** to identify the an account associated with the mobile phone number.

In another embodiment, the payment processing server **110** queries a register of data points **414**, described in greater detail below. Responsive to the query, the payment processing server **110** receives the account information associated with the phone number of the mobile device **102** or the identity of the mobile enablement center **106** associated with the mobile device's **102** phone number. In one embodiment, the payment processing server **110** queries the mobile enablement center **106**. Responsive to receiving the query, the mobile enablement center **106** queries a register of payment processing server **108** to retrieve the account information associated with the mobile device's **102** phone number. Once the payment processing server **110** receives the appropriate account information, the payment processing server **110** communicates with the mobile enablement center **106** associated with the mobile device's **102** phone number and sends a transaction authorization request to the mobile device **102**. In one embodiment, the payment processing server **110** sends a transaction authorization to the merchant **102**. As described in greater detail below, upon receiving a positive transaction authorization from mobile device **102** or the merchant **104**, the payment processing server **110** initiates a transaction with an financial institution **116** associated with the account number.

As described above, the payment processing server **110** can identify an account associated with the mobile phone number **102**. In one instance, more than one account may be identified as associated with the mobile phone number. In such an embodiment, the payment processing server **110** queries a mobile enablement center **106**. The mobile enablement center **106** identifies an account associated with more than one account such as virtual accounts or real accounts that are identified as associated with the mobile phone number. In such an instance, additional logic can be used by the mobile enablement center **106** to identify an account from a list of possible accounts associated with the mobile phone number. For example, a user can provide that a debit account should be used for purchases under a certain dollar amount, such as $5. In another embodiment, the customer can associate the use of particular accounts when executing a transaction with a particular merchant. Thus, the payment processing server **110** can identify a debit account, if the merchant ID is associated with a retail merchant.

In one embodiment, the payment processing server **110** authenticates the merchant responsive to receiving the transaction information from the merchant. For example, the merchant can be authenticated if the merchant confirms the merchant ID or the customer mobile phone number initiating the transaction. In one instance, the payment processing server **110** identifies an account associated with the merchant once the authentication process is completed.

In one embodiment, the payment processing server **110** sends **208** an authorization request to the mobile device **102** that initiated the transaction request. For example, the payment processing server **110** sends a COMM, an SMS message or an email to the customer phone number or the email address initiating the transaction. In one embodiment, the payment processing server **110** can send **208** an account name and number to the mobile device **102** along with the authorization request. In another embodiment, the customer can provide a phone number associated with a customer account and a different communications phone number. For example, the customer initiating a transaction can provide an account phone number by initiating a communication from a different phone number. In such an instance, the customer can use an application executing on the communications mobile device **102** to initiate the transaction or use COMM messaging. In such an instance, the payment processing server **110** sends **208** an authorization request to the communications phone number, wherein the customer can provide an authorization associated with the account phone number. This could apply to a customer borrowing someone else's mobile device to perform his or her own transaction.

In one embodiment, the payment processing server **110** receives **210** an authorization from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **210** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

In one embodiment, the payment processing server **110** executes **212** a transaction with a financial institution. For example, the payment processing server **110** identifies a financial institution associated with the customer's account and a financial institution associated with the merchant's account, wherein the execution of the transaction comprises of debiting the purchase amount from the customer's account and crediting the purchase amount to the merchant account. In one embodiment, additional fees applied by financial institutions **116**, payment processing servers **110**, mobile enablement centers **106** can be applied to the purchase amount.

In one embodiment, the payment processing server **110** sends **214** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described below in reference to FIG. **3** can be used to send **214** the confirmations. In one embodiment, the payment processing server **110** sends the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the payment processing server **110** sends **214** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc. In another instance the payment processing server **110** sends **214** the transaction confirmation via COMM to the merchant's mobile device if one was identified by merchant as preferred delivery mechanism for confirmations

FIG. **3** is a high-level block diagram illustrating a functional view of a typical computer system **300** for use as one of the entities illustrated in the computing environment of FIG. **1** according to one embodiment. It is noted that the computing machine **300** may also be a system or part of a system, e.g., two or more machines operating together or one or more machines operating with one or more other devices.

FIG. **3** illustrates components of a machine able to read instructions from a machine-readable medium and execute them in one or more processors and/or controllers. Specifically, FIG. **3** shows a diagrammatic representation of a machine within which mobile payment device instructions **324** (e.g., software code) can be executed to perform anyone or more of the methodologies discussed herein. In alterative embodiments, the machine operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server machine or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment.

The machine may be a server computer, a client computer, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a smartphone, a web appliance, a network router, switch or bridge, or any machine capable of executing instructions **324** (sequential or otherwise) that specify actions to be taken by that

machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute instructions **324** to perform anyone or more of the methodologies discussed herein.

The example computer machine **300** includes a processor **302** (e.g., a central processing unit (CPU), or group of processors, or a group of processing machines, a graphics processing unit (GPU), a digital signal processor (DSP), one or more application specific integrated circuits (ASICs), one or more radio-frequency integrated circuits (RFICs), or any combination of these), a memory **304**, including a main memory and a static memory, a network interface device **320** capable of interacting with a network **310**, an input/output device **312** (e.g., a keyboard, a cursor control device, a plasma display panel (PDP), a liquid crystal display (LCD), a projector, or a cathode ray tube (CRT)) and a storage unit **316** configured to communicate with each other via a bus.

The storage unit **316** includes a machine-readable medium **322** on which is stored mobile payment device instructions **324** (e.g., software) embodying any one or more of the methodologies or functions described herein. The mobile payment instructions **224** (e.g., software) may also reside, completely or at least partially, within the main memory **304** or within the processor **302** (e.g., within a processor's cache memory) during execution thereof by the computer system **300**, the main memory **304** and the processor **302** also constituting machine-readable media.

The external storage **317** includes a machine-readable medium on which mobile device or merchant information can be stored. In one embodiment, the machine **300** can access the external storage **317** via a communications links, as described above. In an embodiment, all components of the machine **300** can access the storage medium **317**.

While machine-readable medium **322** is shown in an example embodiment to be a single medium, the term "machine-readable medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, or associated caches and servers) able to store instructions (e.g., mobile payment device instructions **324**). The term "machine-readable medium" shall also be taken to include any medium that is capable of storing instructions (e.g., mobile payment device instructions **324**) for execution by the machine and that cause the machine to perform any one or more of the methodologies disclosed herein. The term "machine-readable medium" includes, but not be limited to, data repositories in the form of solid-state memories, optical media, and magnetic media.

The mobile payment device instructions **324** (e.g., software) may be transmitted or received over the network **310** via the network interface device **320**. In one embodiment, the network **310** is the Internet. The network **310** can also utilize dedicated or private communications links that are not necessarily part of the Internet. In one embodiment, the network **114** uses standard communications technologies and/or protocols. Thus, the network **114** can include links using technologies such as Ethernet, Wi-Fi (802.11), integrated services digital network (ISDN), digital subscriber line (DSL), asynchronous transfer mode (ATM), etc. Similarly, the networking protocols used on the network **114** can include multiprotocol label switching (MPLS), the transmission control protocol/Internet protocol (TCP/IP), the hypertext transport protocol (HTTP), the simple mail transfer protocol (SMTP), the file transfer protocol (FTP), etc. In one embodiment, at least some of the links use mobile networking technologies, including general packet radio service (GPRS), enhanced data GSM environment (EDGE), code division multiple access 2000 (CDMA2000), and/or wide-band CDMA (WCDMA). The data exchanged over the network **114** can be represented using technologies and/or formats including the hypertext markup language (HTML), the extensible markup language (XML), the wireless access protocol (WAP), the short message service (SMS) etc. In addition, all or some of links can be encrypted using conventional encryption technologies such as the secure sockets layer (SSL), Secure HTTP and/or virtual private networks (VPNs). In another embodiment, the entities can use custom and/or dedicated data communications technologies instead of, or in addition to, the ones described above.

The example computer machine **300** includes a mobile network enablement unit **325** which includes the logic software (SLEE—Service Logic Execution Environment) and hardware for connecting to connect, control and communicate with any mobile network operator's node, any messaging node (such as a short message service center (SMSC), a multimedia message service center (MMSC), mail transport/transfer agent (MTA), wireless access protocol (WAP), database (DB), (session description protocol) SDP, service control point (SCP), mobile switching center (MSC), central office (CO) for wired communications, service switching point (SSP), authentication, authorization and access/accounting (AAA), gateway GPRS (general packet radio service) support node (GGSN), combined GPRS node (CGSN), packet data servicing node (PDSN), or any other node that may exists in the operator network regardless of the technology used (CDMA, WCDMA, iDEN, GSM, 2G, 3G, 4G, or future revisions of the wireless communications system, Bluetooth, WiFi, WiMax, Radio (short wave or other), infrared or any other communication method or protocol known in the art). Mobile network enablement unit **325** supports all communication protocols and standards including but not limited to instant messaging service (IMS), signaling system 7 (SS7), internet protocol (IP), transport/transmission control protocol (TCP), transaction capabilities application part (TCAP), intelligent network application protocol (INAP), mobile application part/multiple access protocol (MAP), CS1, CS2, CS3, CS4, common alerting protocol version 1 (CAP v1), CAPv2, CAPv3, CAPv4, all wireless intelligent network (WIN) standards, all intelligent network (IN) standards and all advanced intelligent network (AIN) standards, etc. In one embodiment, the mobile network enablement unit **325** communicates with a mobile operator network **311**. As described in greater detail above, the mobile operator network **311** includes CDMA, WCDMA, iDEN, GSM, 2G, 3G, 4G, or future revisions of the wireless communications system.

Referring now to FIG. **4**, it illustrates a high-level block diagram of a computing environment for using a mobile device to initiate a transaction according to one embodiment. The computing environment may include a mobile device **102**, a mobile enablement center **106**, a register of payment processing servers **108**, a payment processing server **110**, a merchant **104**, a service data point **412**, a register of service data points **414** and a financial institution **116**.

FIG. **5** is a flowchart illustrating a method of using a mobile device to initiate a transaction using a service data point according to one embodiment. For the purposes of discussion, FIGS. **4** and **5** are discussed concurrently below.

As described in greater detail above, the mobile device **102** initiates a transaction request by sending a merchant ID to the mobile enablement center **106** or the payment processing server **110**. The payment processing server **110** receives **502** the merchant ID and sends **504** a transaction information request to the merchant associated with the merchant ID. As

described above, any communications method (COMM) known in the art can be used to communicate with the merchant **104**. For example, the payment processing center can send an SMS message, an e-mail message etc to a phone number or an email address associated with the merchant **104**. In one embodiment, the merchant ID can be associated with a merchant's unique point-of-sale terminal. In such an instance, the payment processing server **110** can send a communication to the point the particular point-of-sale terminal. The payment processing server **110** can also use the commonly known ISO8583 interface to communicate with the point of sale terminal.

Service data point (also referred to as SDP) is a computing machine with, for example, all the components described above in **300**, that telecommunication operators normally use to store service logic and subscriber account balances, subscriptions, services, expiration of service dates, etc. SDPs have multiple names in different operator and vendor environments, for the purpose of this disclosure SDP refers to any and all of those nodes equivalent in function as described herein.

In one embodiment, the SDP can be used for banking, financial, investment and/or insurance operations such as keeping track of account balances, debiting accounts, crediting accounts and transferring of account funds from one account to another. A centralized SDP or SDP Register can be used to provide routing information to signals destined to a certain SDP. In an embodiment, an SDP register can be under the control, jurisdiction (auspices) of a governmental or consortium body that would regulate its functions and management.

In one embodiment the SDP communicates with financial institutions **116**, ATM machines, point of sale terminals, a mobile enablement center **106** and/or a merchant **104** for the purpose of processing point of sale transactions with financial institutions or payment processing servers **110**. For example SDP will support any standard data communication protocol and data security standards such as, but not limited to, International Standards Organization (ISO) 8583, simple object access protocol (SOAP)/extensible markup language (XML), SOAP, hypertext transfer protocol (HTTP), secure sockets layer (SSL), etc.

In one embodiment, the payment processing server **110** identifies **504** a service data point (SDP) responsive to a phone number provided by the mobile device **102**. The phone number is a customer phone number associated with the customer's banking account that is controlled by SDP. A service data point **412** is a database where customer phone numbers are stored in addition to customer account information, and where the customer's account information can be retrieved based on its associated with the provided phone number. In one embodiment, the service data point **412** can be used to control financial institution accounts.

In one embodiment, the payment processing server cannot identify an appropriate SDP based on the provided account phone number. In such an instance, the payment processing system sends an interrogation request to the registry of SDPs **414** to identify **504** an SDP associated with the customer's account phone number. The registry of SDPs **414** provides the routing information to an SDP **412** associated with the customer's banking account.

Once an appropriate SDP **412** is identified, the payment processing server interrogates the SDP to receive **506** account information associated with the customer's phone number. The SDP **412** can retrieve account information associated with the customer's phone number.

As described above, the payment processing server **110** sends **508** a transaction information request to the merchant indentified by the merchant ID. Responsive to the request, the merchant can send transaction information to the payment processing server. In one embodiment, the payment processing server receives **510** the transaction information from the merchant via communications means known in the arts. As described above, the transaction information can include the total purchase price for the items the customer wants to purchase, an account number associated with the merchant, the mobile phone number provided by the customer etc. The merchant **104** can use any communications method (COMM) known in art to provide the transaction information to the payment processing server **110**. In one embodiment, the merchant can enter the total purchase amount on a point-of-sale terminal's keypad.

As described above, in one embodiment, the payment processing server **110** sends **512** an authorization request to the mobile device **102** that initiated the transaction request. For example, the payment processing server **110** sends a COMM, an SMS message or an email to the customer phone number or the email address initiating the transaction. In one embodiment, the payment processing server **110** can send **512** an account name and number to the mobile device **102** along with the authorization request. In another embodiment, the customer can provide a phone number associated with a customer account and a different communications phone number. For example, the customer initiating a transaction can provide an account phone number by initiating a communication from a different phone number. In such an instance, the customer can use an application executing on the communications mobile device **102** to initiate the transaction, or do it using COMM messaging. In such an instance, the payment processing server **110** sends **512** an authorization request to the communications phone number, wherein the customer can provide an authorization associated with the account phone number.

In one embodiment, the payment processing server **110** receives **514** an authorization message from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **514** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (or a one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

Once a correct authorization code e.g., a PIN is received from the mobile device **102**, the payment processing server executes the requested transaction with the SDP **412**. The

SDP **412** updates the account information associated with the customer. The payment processing server **110** sends a transaction confirmation to the mobile device **102** and the merchant **104**. As described above, in one embodiment, the payment processing server **110** sends **518** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described above can be used to send **518** the confirmations. In one embodiment, the payment processing server **110** sends **518** the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the payment processing server **110** sends **518** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc.

FIG. **6**, illustrates a high-level block diagram of a computing environment for using a mobile device to execute a transaction according to one embodiment. The computing environment may include a mobile device **102**, a payment processing server **110**, a merchant **104** and a financial institution **116**.

FIG. **7** is a flowchart illustrating a method of using a mobile device to initiate a transaction using a service data point according to one embodiment. For the purposes of discussion, FIGS. **6** and **7** are discussed concurrently below.

In one embodiment of the system and method described below, the point of sale is initiated by the merchant. In one embodiment, a point of sale terminal associated with the merchant **104** is used to enter and send point of sale information such as a transaction amount, a communications phone number and an account phone number. An account phone number is a phone number associated with a financial institution. For example, the customer can preset that a particular phone number is associated with a particular account with a financial institution. The account can be a credit account, a debit account, a savings account, a payroll account, etc. A communications phone number can be the phone number associated with the customer. In another instance, the communications phone number is different from an account phone number, allowing a customer to use a borrowed phone to execute a transaction. For example, if a customer realizes that he or she lost or forgot his or her mobile phone, the customer can borrow someone else's phone by requesting that a communication be sent to the phone number associated with the borrowed phone. In other embodiments, the customer can provide a communications email address or an account email address wherein, the email account is associated with a financial institution's account for the customer.

In one embodiment, the payment processing server **110** receives **702** the point of sale information from the merchant **104**. The payment processing server **110** sends **704** an authorization request to the communications phone number provided by the merchant **104**. As described above, in one embodiment, the payment processing server **110** sends **704** an authorization request to the communications phone number or the account phone number as provided by the customer. In one embodiment, the payment processing server **110** sends a COMM, an SMS message or an email to the phone number or the email address initiating the transaction. In one embodiment, the payment processing server **110** can send **704** an account name and number to the mobile device **102** along with the authorization request. For example, if the customer has associated several credit or debit accounts with an account phone number, the payment processing server **110** can provide a listing of all the accounts available to the customer. In such an instance the payment processing server **110** opens a data session to the mobile device **102** and provides a menu to choose from wherein the customer can choose the account to execute the transaction with. In another embodiment, the payment processing server **110** uses a USSD menu option if available in the network or a WAP push message with several links denoting various accounts, or communicate to a client on the mobile device **102**. Also, in such an instance, the customer can enter an authorization PIN for an account the customer wishes to use to execute the purchase. In another embodiment, the payment processing system requests one PIN even if the customer has associated several accounts with the account phone number. In such an instance, the customer can enter the authorization PIN for the account the customer wants to use to execute the purchase. The payment processing server **110** can identify a credit or a debit account based on whether the authorization PIN matches one of accounts associated with the account phone number.

In one embodiment, the customer can enter and send a message to the payment processing server **110** to authorize the transaction. The payment processing server **110** receives **706** the authorization from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated with the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, a one-time password (or a one time use PIN which expires on first use) or PIN can be used by a customer when using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **706** the authorization PIN from the customer through a communications network.

Responsive to the customer sending the authorization, the payment processing server **110** receives **706** the authorization from the mobile device **102**. As described in greater detail above, the payment processing server executes **708** the point of sale transaction with financial institutions associated with the customer and the merchant **104**. Once the transaction is executed **708**, the payment processing server sends a confirmation to the merchant **104**, the communication and the account phone number associated with the customer. As described above, in one embodiment, the payment processing server **110** sends **710** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described above can be used to send **710** the confirmations. In one embodiment, the payment processing server **110** sends **710** the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is

different than a phone number associated with the transaction account, the payment processing server **110** sends **710** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc.

Referring now to FIG. **8**, it illustrates a high-level block diagram of a computing environment for using a mobile device to execute a transaction associated with a sub-account according to one embodiment. The computing environment may include a mobile device **102**, an SDP **412**, an account associated with the mobile phone number **810** and a sub-account associated with the mobile phone number **812**.

FIG. **9** is a flowchart illustrating a method of using a mobile device to execute a transaction associated with a sub-account according to one embodiment. For the purposes of discussion, FIGS. **8** and **9** are discussed concurrently below.

As described in greater detail above, the mobile device **102** or the merchant **104** can initiate a transaction request by sending a merchant ID and an account phone number to a service data point (SDP) **412**. In one embodiment, the SDP receives **902** the transaction request either from the merchant **104** or from the mobile device **102**. In one embodiment, the SDP is interrogated **904** to determine if the received account phone number is associated with a sub-account. A sub-account **812** is associated with the a parent account **810** wherein the sub-account may have limited access to the funds available to the parent account **810** or the account associated with the mobile phone number. If the SDP determines that the account phone number is associated with a sub-account, the SDP provides that a sub-account criteria is matched **906**.

In other embodiments, the sub-account criteria can be matched **906** in other ways. For example, a phone number can be associated with a sub-account. In such an instance, if a communications phone number matches the sub-account **812** criteria, the SDP executes **912** a transaction with the sub-account responsive to receiving the appropriate authorization. In other embodiments, an authorization PIN can be associated with a sub-account. If the sub-account criteria are met, the SDP sends an authorization request to one or more of the communications phone number, a phone number associated with the sub-account or a phone number associated with the parent account **810**. For example, the SDP or the payment processing server **110** can send **908** an authorization request to the account phone number associated with the parent account **810** or the phone number associated with the sub-account, or both. As such, a customer can create a sub-account for a family member, such that the customer's children or other family members can make certain purchases using their own mobile device. Similarly, in an embodiment wherein the authorization request is sent to a phone number associated with the parent account **810**, the parent can provide real-time approval or rejection of certain purchases initiated by the sub-account holder.

As described above, in one embodiment, the payment processing server **110** sends **908** an authorization request to an appropriate mobile device **102** including the mobile device **102** that initiated the transaction request or to a phone number associated with the parent account **810**. For example, the payment processing server **110** sends an SMS message or an email the phone numbers or the email address provided. In one embodiment, the payment processing server **110** can send **908** an account name and number to the appropriate mobile device **102** along with the authorization request. In another embodiment, the customer can provide a phone number associated with a customer account and a different communications phone number. For example, the customer initiating a transaction can provide an account phone number by initiating a communication from a different phone number. In such an instance, the customer can use an application executing on the communications mobile device **102** to initiate the transaction or use COMM messaging. In such an instance, the payment processing server **110** sends **908** an authorization request to the communications phone number, wherein the customer can provide an authorization associated with the account phone number.

The SDP can receive **910** the authorization from the sub-account phone number, the communications phone number or the phone number associated with the parent account **810**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **910** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (or a one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

The SDP can initiate an execution of the transaction between the customer and the merchant **104**. If the SDP does not receive an appropriate authorization or a sub-account criteria match, the SDP executes **914** the transaction with the parent-account **810**. As described in greater detail above, a transaction confirmation is sent to the merchant, the communications phone number, the account phone number or the sub-account phone number.

FIG. **10** is a high-level block diagram that illustrates a computing environment for using a payroll card to execute a transaction according to one embodiment. The computing environment may include a mobile device **102**, a mobile enablement center **106**, a register of payment processing servers **108**, a payment processing server **110**, a merchant **104**, a service data point **112**, a register of service data points **114** and a financial institution **116**.

In one embodiment the SDP could control an aggregate account (also referred to as a Nostro Account) in a bank that includes multiple sub accounts that can represent payroll accounts. Such payroll accounts could be used for those that cannot establish an account on their own because of lack of sufficient funds or lack of good credit. Such aggregate accounts could be accessed by any payment processing server **110** or SDP if they are associated with a mobile phone number. One such subaccount in an aggregate account can have multiple virtual accounts. For example a worker with no bank account would ask employer to use such subaccount for direct deposit of payroll. The subaccount would be associated with the workers mobile phone number. The worker would be able to create multiple virtual sub-subaccounts on the SDP and

move funds to those sub-subaccounts. Each sub-subaccount would be associated with a mobile phone and could be accessed by phone with the aid of any payment processing server **110** or mobile enablement center **106**. In one embodiment the SDP can take the place or perform the functions of the mobile enablement center. In one embodiment the SDP can control fund transfer between banks, phone account numbers and between merchants.

FIG. **11** is a flowchart illustrating a method of using a payroll card to execute a transaction according to one embodiment. For the purposes of discussion, FIGS. **10** and **11** are discussed concurrently below.

In the embodiment discussed in reference to FIGS. **10** and **11**, the point of sale transaction is initiated by a merchant **104** or a mobile device **102**, wherein the account phone number is associated with a payroll card **1002**. A payroll card **1002** can be a debit card associated with a payroll account. An employer of the customer using the payroll card can deposit payroll checks in the payroll account. For example, instead of giving the customer a weekly, bi-weekly or monthly payroll check which can be either cashed or deposited, the employer can make weekly, bi-weekly or monthly payroll deposits to the payroll account, such that the employer would not have to issue new payroll checks each payroll cycle. Such a system is beneficial because it reduces the employer's cost of issuing checks. Additionally such a system is beneficial to employees because they have access to an account associated with a card which can be used to make purchases without opening additional accounts or a new line of credit with another financial institution. Additionally, each payroll account can be associated with a payroll trust account. A payroll trust account is an aggregate of accounts used by the employer to make deposits to each individual payroll account associated with an employee. The payroll trust account generally carries a float and cannot be closed. As described in greater detail below, an additional benefit of the system and method described herein is to allow customers to borrow funds from the trust account if the funds in the their customer payroll accounts are depleted. The payroll trust account can withhold money due to the employee in the next payroll period. The withheld money can be a portion of the borrowed money, the entirety of the borrowed money or the entirety of the borrowed money in addition to fees and interests.

In one embodiment, the payment processing server receives **1102** a request to execute a transaction from an account associated with the payroll card **1002**. For example, a merchant can swipe or enter the account number associated with the payroll card on a point of sale terminal. In such an instance, the point of sale terminal can receive a firmware update to enable a customer to use a payroll account card to execute a purchase. In another embodiment, a mobile device can be used to initiate a point of sale transaction. As described above, the mobile device can send an account phone number and a merchant identification to a service data point (SDP) **412** or to a mobile enablement center **106**. In another embodiment, as described above, the customer can borrow a mobile computing device to initiate a point of sale transaction.

Upon receiving the request, the SDP sends **1104** and receives **1106** appropriate authorization information to a mobile phone number associated with the payroll account or communications phone number. As described above, in one embodiment, the SDP **412** sends **1104** an authorization request to the mobile device **102** associated with the payroll account. For example, the SDP **412** sends an COMM, SMS message or an email to the customer phone number or the email address associated with the payroll account. In one embodiment, the SDP **412** can send **1104** an account name and number to the mobile device **102** along with the authorization request. In another embodiment, the payment processing server can send **1104** authorization request to communications phone number different from the account phone number associated with the payroll account. For example, a communications phone number can be provided in the communication received **1102** providing payroll account information to execute a transaction. In such an instance, the customer can use an application executing on a mobile device **102** associated with the communications phone number to initiate the transaction.

In one embodiment, the SDP **412** receives **1106** an authorization from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the SDP **412** receives **1106** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (or a one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

An SDP logic identifies whether the payroll account has enough funds **1108** to execute the requested transaction. If so, the SDP executes **1112** the transaction with a bank associated with the payroll card. If the SDP determines that the payroll account does not have sufficient funds, the SDP executes **1110** a transaction with the payroll trust account. Once the transaction is complete, a transaction confirmation is send to the merchant and the mobile device associated with the payroll account. In one embodiment, the SDP **412** sends **1114** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described above can be used to send **1114** the confirmations. In one embodiment, the SDP **412** sends **1114** the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the SDP **412** sends **1114** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc.

While particular embodiments and applications of the present invention have been illustrated and described herein, it is to be understood that the invention is not limited to the precise construction and components disclosed herein and that various modifications, changes, and variations may be made in the arrangement, operation, and details of the meth-

ods and apparatuses of the present invention without departing from the spirit and scope of the invention as it is defined in the appended claims.

What is claimed is:

1. A method for conducting a transaction between a merchant and a customer, the customer using a mobile device, the method comprising:

receiving a merchant identifier from the mobile device operated by the customer, the merchant identifier indicating a request to initiate a transaction with a merchant terminal identified by the merchant identifier, wherein the merchant identifier does not indicate a transaction amount for the transaction;

sending, in response to receiving the merchant identifier, a transaction information request to the merchant terminal associated with the merchant identifier;

receiving transaction information from the merchant terminal in response to the transaction information request, the transaction information including the transaction amount for the transaction;

identifying a purchase account associated with the customer and a deposit account associated with the merchant; and

initiating the transaction between the merchant and the customer for the transaction amount received from the merchant terminal and the identified purchase account associated with the customer and the identified deposit account associated with the merchant.

2. The method of claim **1**, wherein the merchant identifier comprises a unique identifier associated with the merchant terminal.

3. The method of claim **1**, wherein the merchant identifier is received from the mobile device by at least one of: an SMS message, an MMS message, an email message, an application, or a phone call.

4. The method of claim **3**, wherein the merchant identifier comprises a number interpreted by an application executing on the mobile device based on a depiction of merchant identification.

5. The method of claim **1**, wherein the merchant terminal is a point-of-sale terminal associated with the merchant.

6. The method of claim **1**, further comprising receiving, from the customer, a pre-set personal identification number for authorizing a transaction from a mobile device unassociated with the customer; determining the mobile device is not associated with the customer; and receiving the pre-set personal identification number from the mobile device.

7. The method of claim **1**, wherein the purchase account associated with a customer is identified based on a phone number associated with the mobile device.

8. The method of claim **1**, wherein the purchase account is identified based on a merchant type or the transaction amount.

9. The method of claim **1**, wherein the purchase account is identified based on an account phone number communicated by the mobile device, wherein a phone number associated with the mobile device is different from the account phone number.

10. The method of claim **1**, wherein initiating a transaction between the merchant and the customer comprises sending instructions to an appropriate financial institutions associated with the purchase account and the deposit account.

11. The method of claim **1**, wherein a mobile enablement center is used to identify an appropriate payment processing server associated with a financial institution.

12. The method of claim **1**, wherein a service data point is used to initiate a transaction between the merchant and the customer.

13. The method of claim **12**, wherein the service data point is identified by a register of service data points responsive to a query to execute a transaction between the customer and the merchant.

14. The method of claim **1**, wherein the merchant terminal is a point of sale terminal is enabled, responsive to a firmware update, to receive a request to initiate a point of sale transaction.

15. A system for conducting a transaction between a merchant and a customer, comprising:

a processor; and

a memory including instructions for execution on the processor, the instructions, when executed on the processor, causing the processor to perform the steps of:

receive a merchant identifier from a mobile device operated by a customer, the merchant identifier indicating a request to initiate a transaction with a merchant terminal identified by the merchant identifier, wherein the merchant identifier does not indicate a transaction amount for the transaction;

send, in response to receiving the merchant identifier, a transaction information request to the merchant terminal associated with the merchant identifier;

receive transaction information from the merchant terminal in response to the transaction information request, the transaction information including the transaction amount for the transaction;

identify a purchase account associated with the customer and a deposit account associated with the merchant; and

initiate the transaction between the merchant and the customer for the transaction amount received from the merchant terminal and the identified purchase account associated with the customer and the identified deposit account associated with the merchant.

16. The system of claim **15**, wherein the merchant identifier comprises a unique identifier associated with the merchant terminal.

17. The system of claim **15**, wherein the merchant identifier is received from the mobile device by at least one of: an SMS message, an MMS message, an email message, an application, or a phone call.

18. The system of claim **17**, wherein the merchant identifier comprises a number interpreted by an application executing on the mobile device based on a depiction of merchant identification.

19. The system of claim **15**, wherein the merchant terminal is a point-of-sale terminal associated with the merchant.

* * * * *

EXHIBIT 2

US010535058B2

(12) **United States Patent**
Afana

(10) **Patent No.: US 10,535,058 B2**
(45) **Date of Patent: *Jan. 14, 2020**

(54) **MOBILE PAYMENT STATION SYSTEM AND METHOD**

(71) Applicant: **Faber Financial, LLC**, Solana Beach, CA (US)

(72) Inventor: **Marwan Monir Afana**, Allen, TX (US)

(73) Assignee: **MOBILE EQUITY CORP.**, Solana Beach, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 452 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/082,425**

(22) Filed: **Nov. 18, 2013**

(65) **Prior Publication Data**

US 2014/0074634 A1 Mar. 13, 2014

Related U.S. Application Data

(63) Continuation of application No. 12/906,989, filed on Oct. 18, 2010, now Pat. No. 8,589,236.
(Continued)

(51) **Int. Cl.**
G06Q 20/20 (2012.01)
G06Q 20/32 (2012.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06Q 20/3223*** (2013.01); ***G06Q 20/20*** (2013.01); ***G06Q 20/40*** (2013.01); ***G06Q 30/00*** (2013.01); ***G06Q 40/00*** (2013.01)

(58) **Field of Classification Search**
CPC G06Q 20/20; G06Q 30/06; G06Q 30/02; G06Q 20/204; G07G 1/12
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,868,391 B1 3/2005 Hultgren
7,873,573 B2 1/2011 Realini
(Continued)

FOREIGN PATENT DOCUMENTS

CN 1614641 A 5/2005
CN 101325748 A 12/2008
(Continued)

OTHER PUBLICATIONS

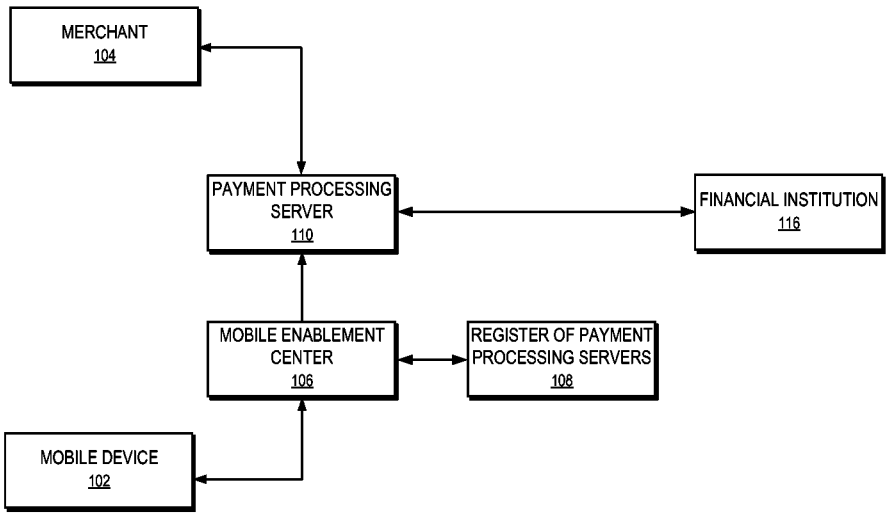
PCT International Search Report and Written Opinion, PCT Application No. PCT/US2010/053059, dated Dec. 23, 2010, 10 pages.
(Continued)

Primary Examiner — Garcia Ade
(74) *Attorney, Agent, or Firm* — Fenwick & West LLP

(57) **ABSTRACT**

A mobile device is used to initiate and execute a transaction between a customer and a merchant. A mobile device is used to initiate a point of sale transaction, wherein a merchant ID is sent to a payment processing server. Responsive to receiving a communication from the mobile device, the payment processing server requests transaction information from the merchant, wherein the merchant is identified based on the provided merchant ID. The merchant can provide transaction information such as the total sale amount to the payment processing server. The payment processing server can authenticate the customer and initiate a purchase transaction with the appropriate financial institutions associated with the customer and the merchant. The payment processing server can send a confirmation of the executed transaction to the merchant and the mobile device.

30 Claims, 11 Drawing Sheets



Related U.S. Application Data

(60) Provisional application No. 61/279,322, filed on Oct. 19, 2009.

(51) **Int. Cl.**

G06Q 20/40	(2012.01)
G06Q 30/00	(2012.01)
G06Q 40/00	(2012.01)

(58) **Field of Classification Search**
USPC 705/16
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,032,414	B2 *	10/2011	Payne	G06Q 20/20 235/381
8,073,424	B2	12/2011	Sun et al.	
8,127,999	B2 *	3/2012	Diamond	G06Q 20/04 235/380
2002/0181710	A1	12/2002	Adam et al.	
2005/0101295	A1	5/2005	Rupp et al.	
2007/0255652	A1	11/2007	Tumminaro et al.	
2009/0248537	A1	10/2009	Sarkeshik	
2010/0223145	A1	9/2010	Dragt et al.	
2011/0041180	A1	2/2011	Jakobsson et al.	

FOREIGN PATENT DOCUMENTS

CN	101454795	A	6/2009
WO	WO 2009/065417	A1	5/2009

OTHER PUBLICATIONS

United States Office Action, U.S. Appl. No. 12/906,989, dated Mar. 26, 2013, 11 pages.
United States Office Action, U.S. Appl. No. 12/906,989, dated Jul. 23, 2012, 10 pages.
Chinese First Office Action, Chinese Application No. 201080047191.7, dated Jan. 29, 2013, 7 pages.
Chinese Second Office Action, Chinese Application No. 201080047191.7, dated Nov. 26, 2013, 13 pages.
European Extended Search Report, European Application No. 10825471.5, dated Jun. 4, 2013, 6 pages.
Mexican Office Action, Mexican Application No. MX/a/2012/004585, dated Jun. 4, 2013, 6 pages (with available written translation).
Mexican Office Action, Mexican Application No. MX/a/2012/004585, dated Oct. 21, 2013, 8 pages (with available written translation).
Taiwan Office Action, Taiwan Application No. 099135645, dated Nov. 29, 2013, 4 pages (with available written translation).
Chinese Third Office Action, Chinese Application No. 201080047191.7, dated Sep. 3, 2014, 12 pages.
Chinese Fourth Office Action, Chinese Application No. 201080047191.7, dated Feb. 13, 2015, 14 pages.
Israel Office Action, Israel Application No. 218998, dated Dec. 8, 2014 (with concise explanation of relevance), 7 pages.
Mexican Office Action, Mexican Application No. MX/a/2012/004585, dated Mar. 25, 2014, 12 pages (with concise explanation of relevance).
Israel Office Action, Israel Patent Application No. 218998, dated Aug. 28, 2016, 4 pages (with concise explanation of relevance).
Canadian Office Action, Canadian Application No. 2,775,586, dated Nov. 30, 2015, 5 pages.
Chinese Board Opinion Office Action, Chinese Application No. 201080047191.7, dated Sep. 28, 2015, 16 pages.
Chinese Board Decision, Chinese Application No. 201080047191.7, dated Dec. 23, 2015, 31 pages.
European Examination Report, European Application No. 10825471.5, dated Oct. 8, 2015, 8 pages.
The Patent Office of the People's Republic of China, Notification of the First Office Action, CN Patent Application No. 2016102113215, dated Dec. 26, 2018, 15 pages.
European Summons to Attend Oral Proceedings Pursuant to Rule 115(1) EPC, European Application No. 10825471.5, dated Nov. 24, 2017, 9 pages.

* cited by examiner

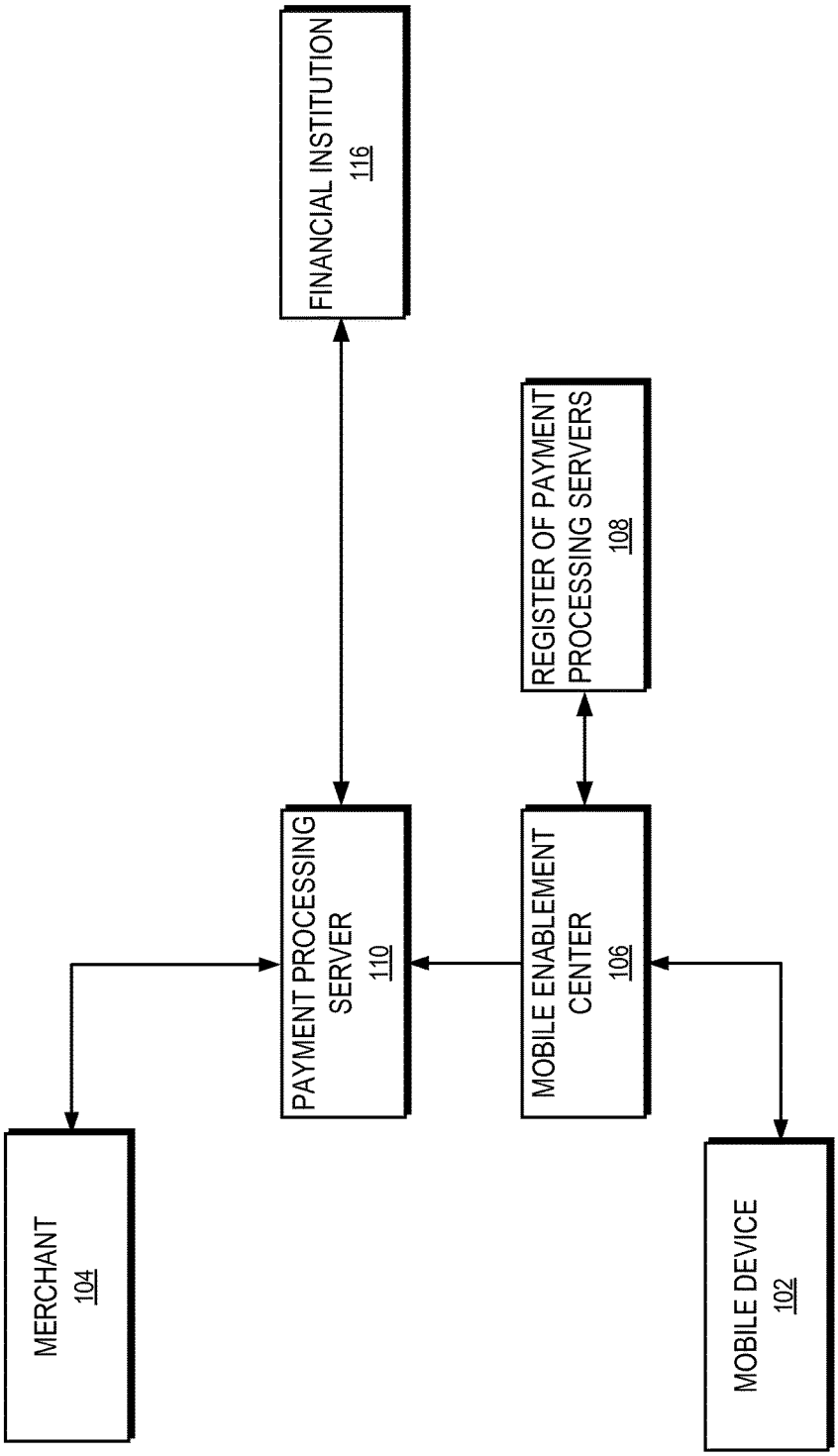

FINANCIAL INSTITUTION
116
REGISTER OF PAYMENT PROCESSING SERVERS
108
PAYMENT PROCESSING SERVER
110
MOBILE ENABLEMENT CENTER
106
MERCHANT
104
MOBILE DEVICE
102

FIG. 1

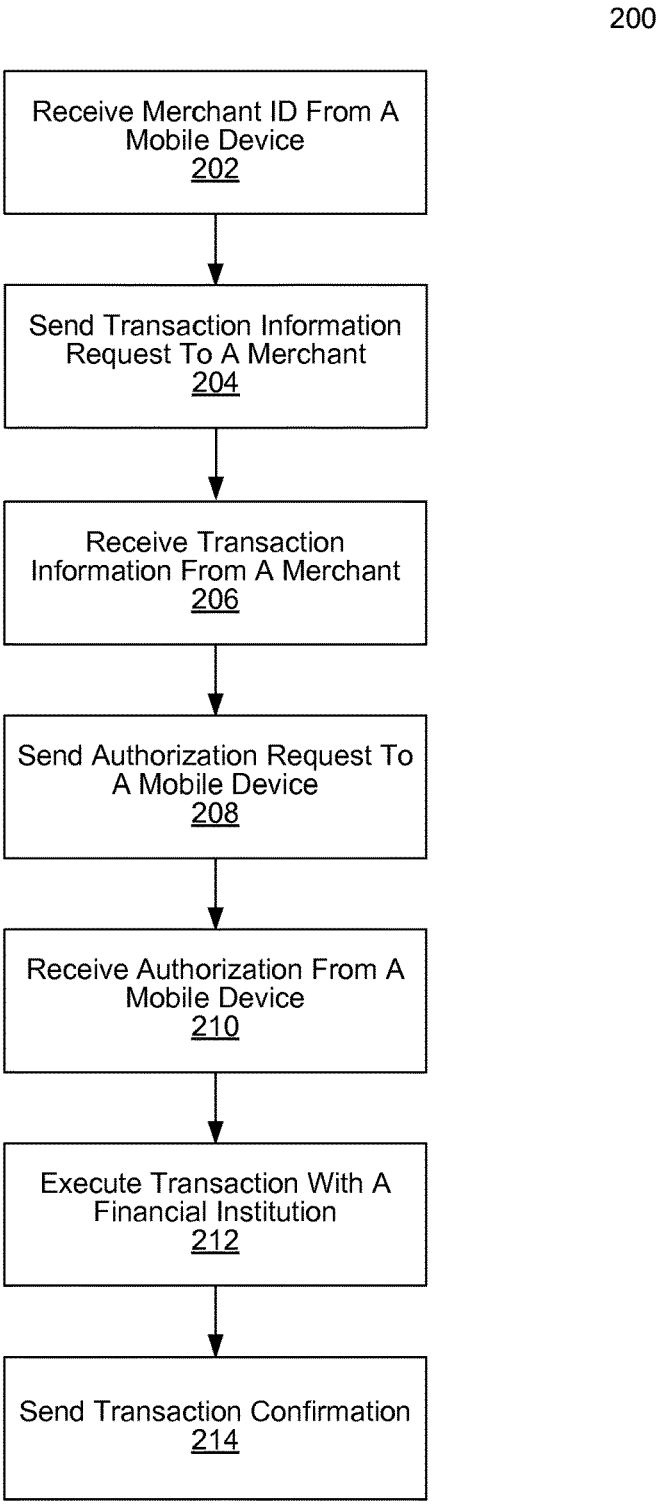

200
Receive Merchant ID From A Mobile Device
202
Send Transaction Information Request To A Merchant
204
Receive Transaction Information From A Merchant
206
Send Authorization Request To A Mobile Device
208
Receive Authorization From A Mobile Device
210
Execute Transaction With A Financial Institution
212
Send Transaction Confirmation
214

FIG. 2

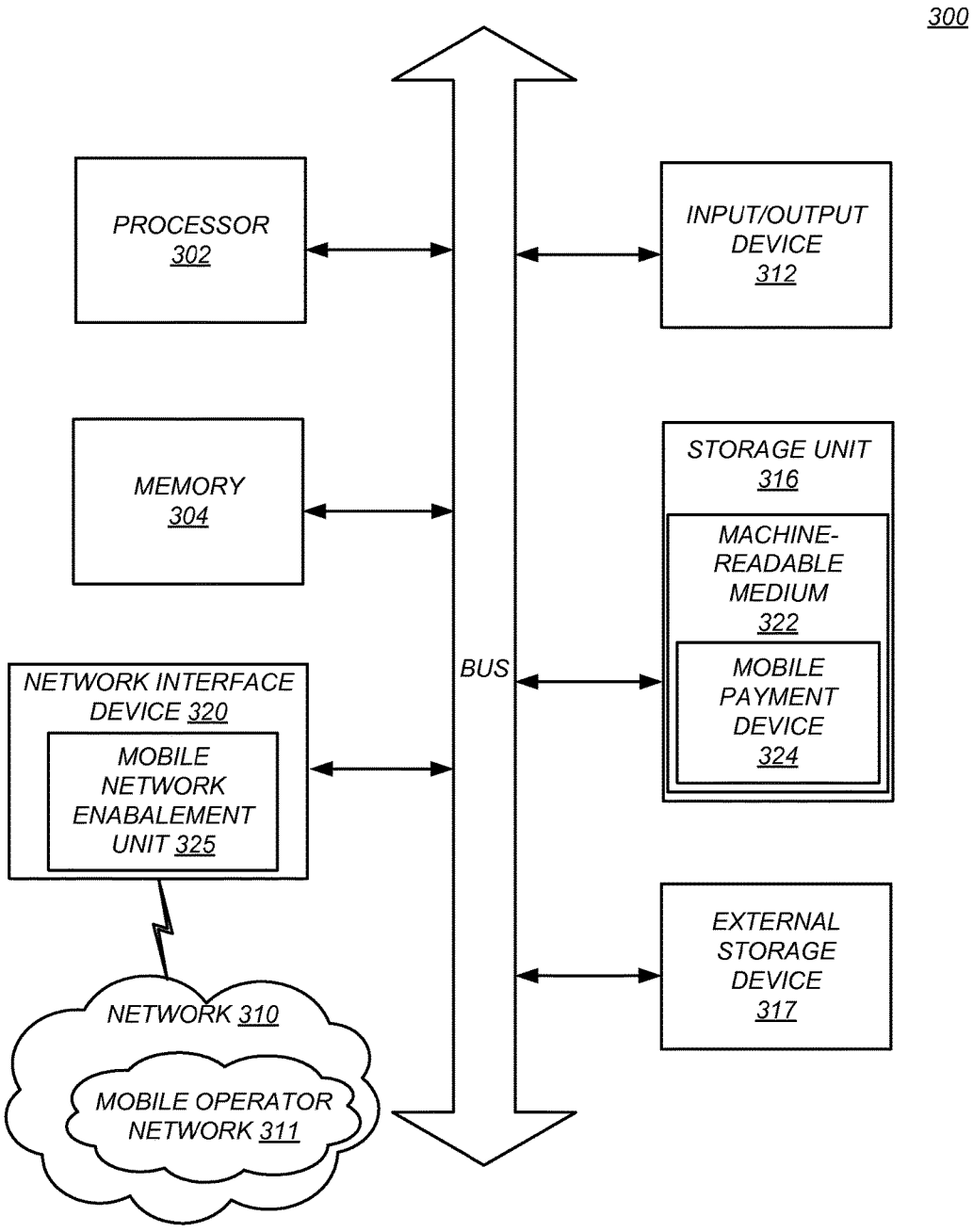

300
PROCESSOR 302
INPUT/OUTPUT DEVICE 312
MEMORY 304
STORAGE UNIT 316
MACHINE-READABLE MEDIUM 322
MOBILE PAYMENT DEVICE 324
BUS
NETWORK INTERFACE DEVICE 320
MOBILE NETWORK ENABALEMENT UNIT 325
EXTERNAL STORAGE DEVICE 317
NETWORK 310
MOBILE OPERATOR NETWORK 311

FIG. 3

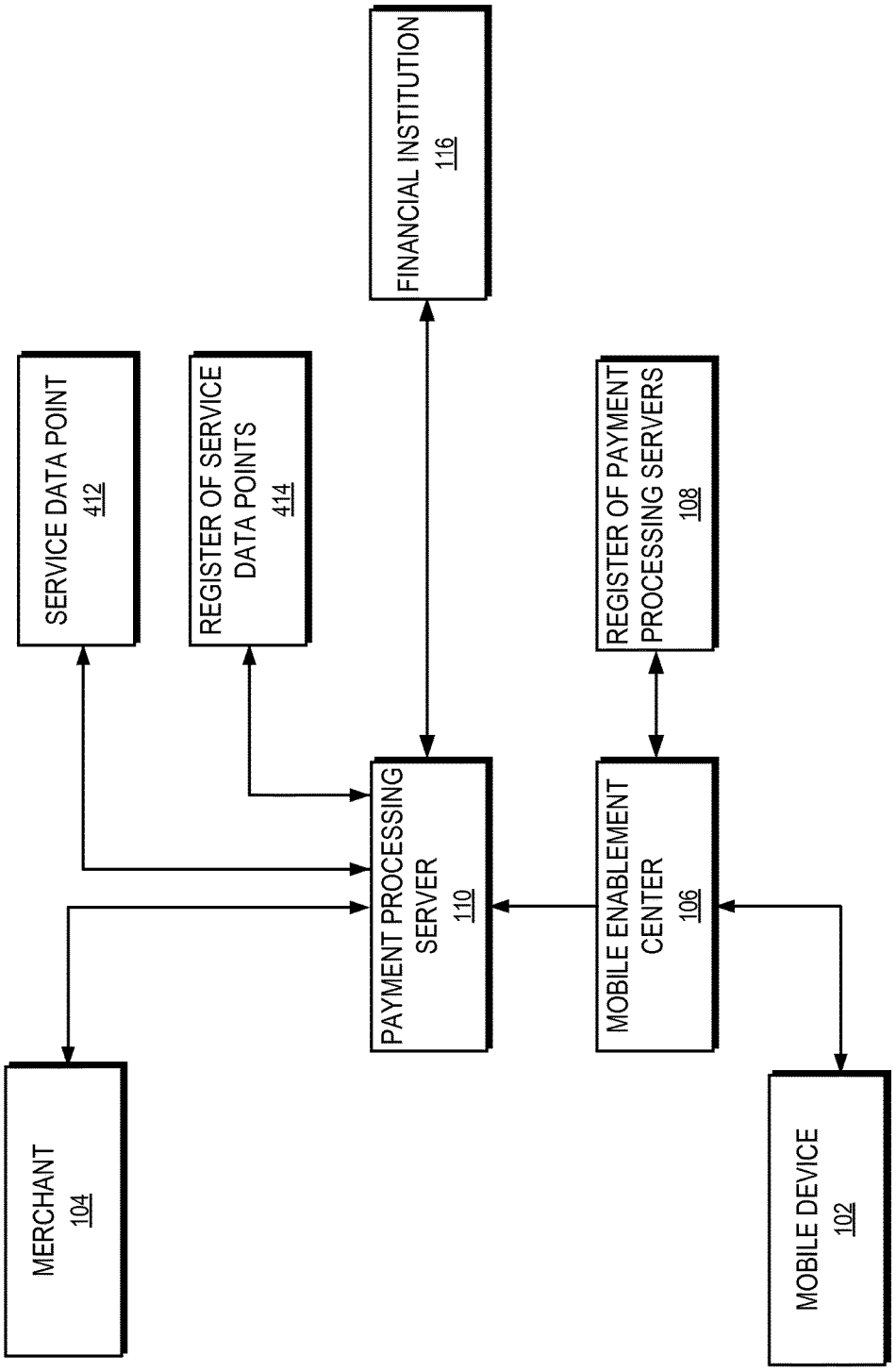

FINANCIAL INSTITUTION
116
SERVICE DATA POINT
412
REGISTER OF SERVICE DATA POINTS
414
REGISTER OF PAYMENT PROCESSING SERVERS
108
PAYMENT PROCESSING SERVER
110
MOBILE ENABLEMENT CENTER
106
MERCHANT
104
MOBILE DEVICE
102

FIG. 4

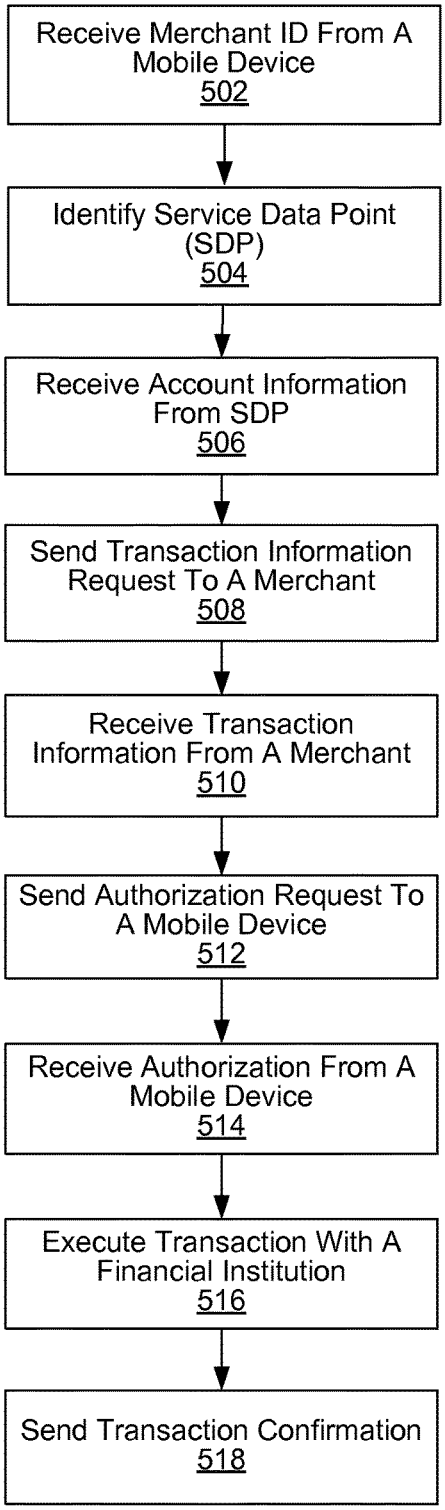

500
Receive Merchant ID From A Mobile Device
502
Identify Service Data Point (SDP)
504
Receive Account Information From SDP
506
Send Transaction Information Request To A Merchant
508
Receive Transaction Information From A Merchant
510
Send Authorization Request To A Mobile Device
512
Receive Authorization From A Mobile Device
514
Execute Transaction With A Financial Institution
516
Send Transaction Confirmation
518

FIG. 5

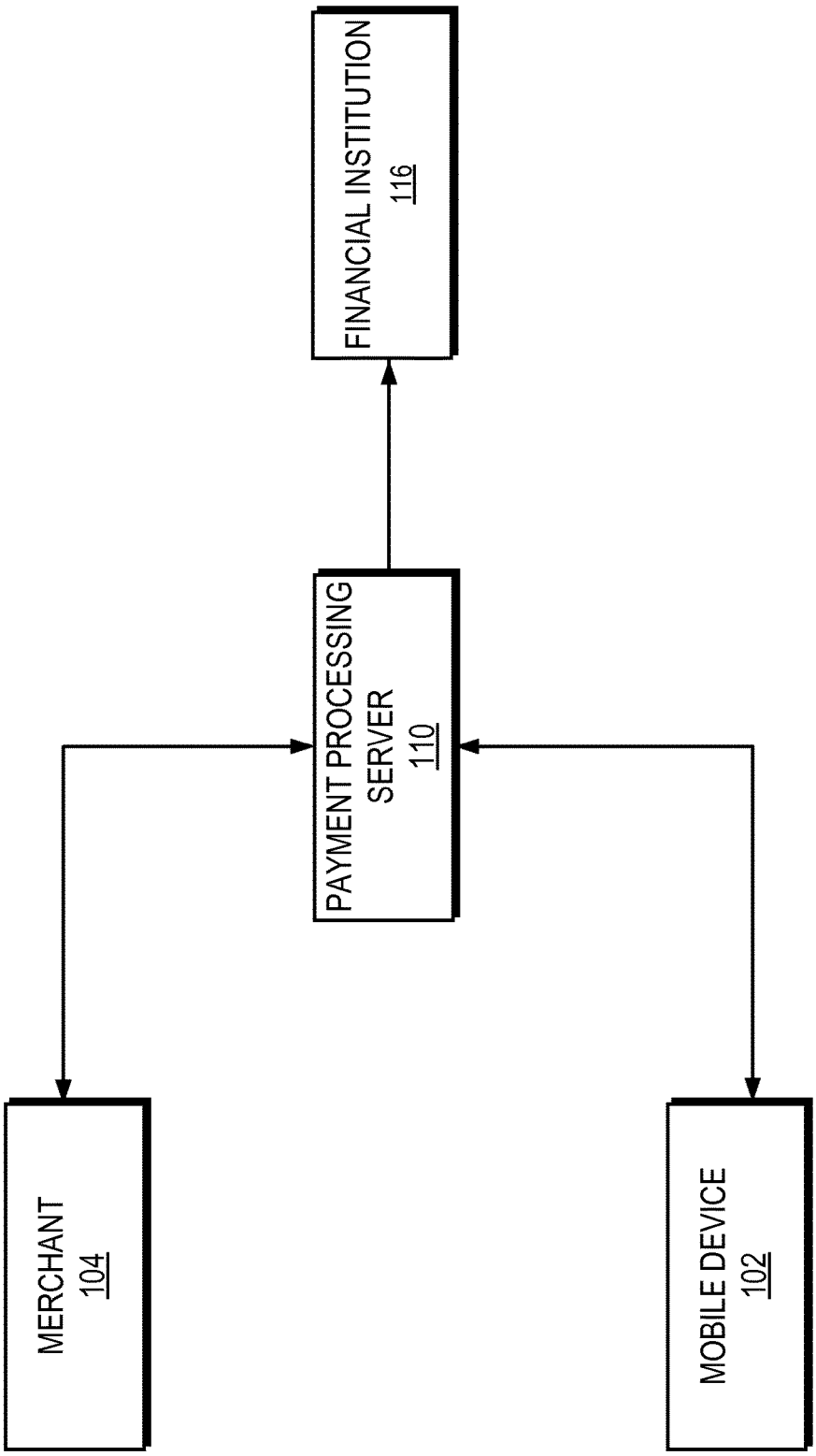

FINANCIAL INSTITUTION
116
PAYMENT PROCESSING SERVER
110
MERCHANT
104
MOBILE DEVICE
102

FIG. 6

700

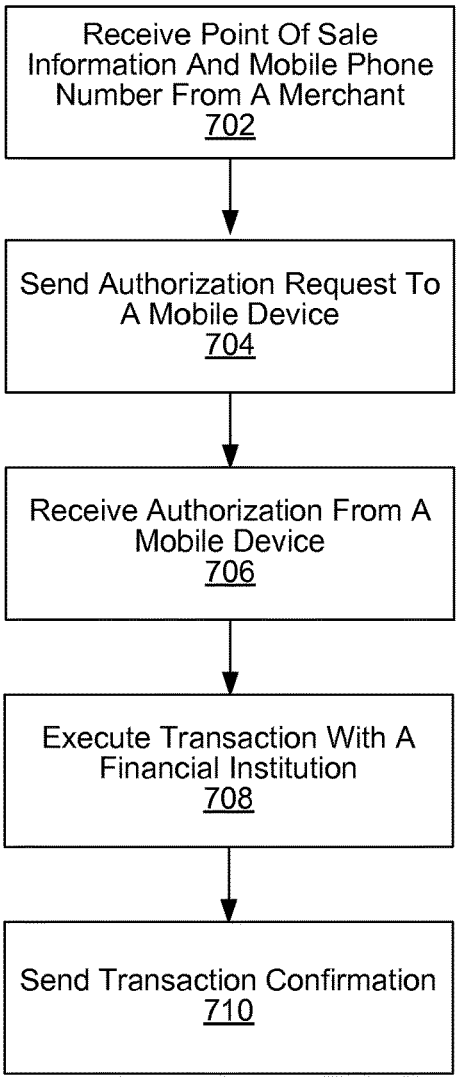

Receive Point Of Sale Information And Mobile Phone Number From A Merchant
702
Send Authorization Request To A Mobile Device
704
Receive Authorization From A Mobile Device
706
Execute Transaction With A Financial Institution
708
Send Transaction Confirmation
710

FIG. 7

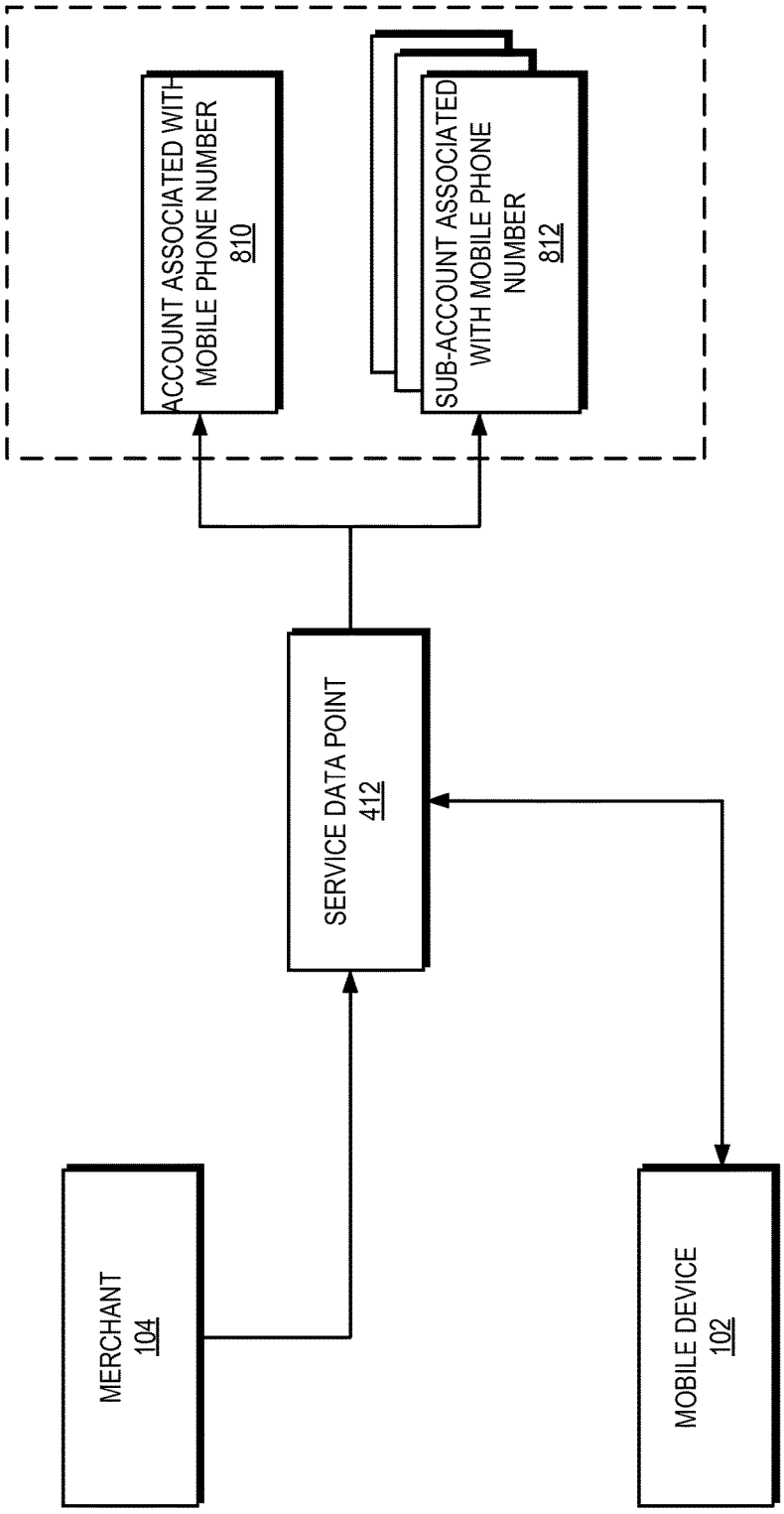

ACCOUNT ASSOCIATED WITH MOBILE PHONE NUMBER 810
SUB-ACCOUNT ASSOCIATED WITH MOBILE PHONE NUMBER 812
SERVICE DATA POINT 412
MERCHANT 104
MOBILE DEVICE 102

FIG. 8

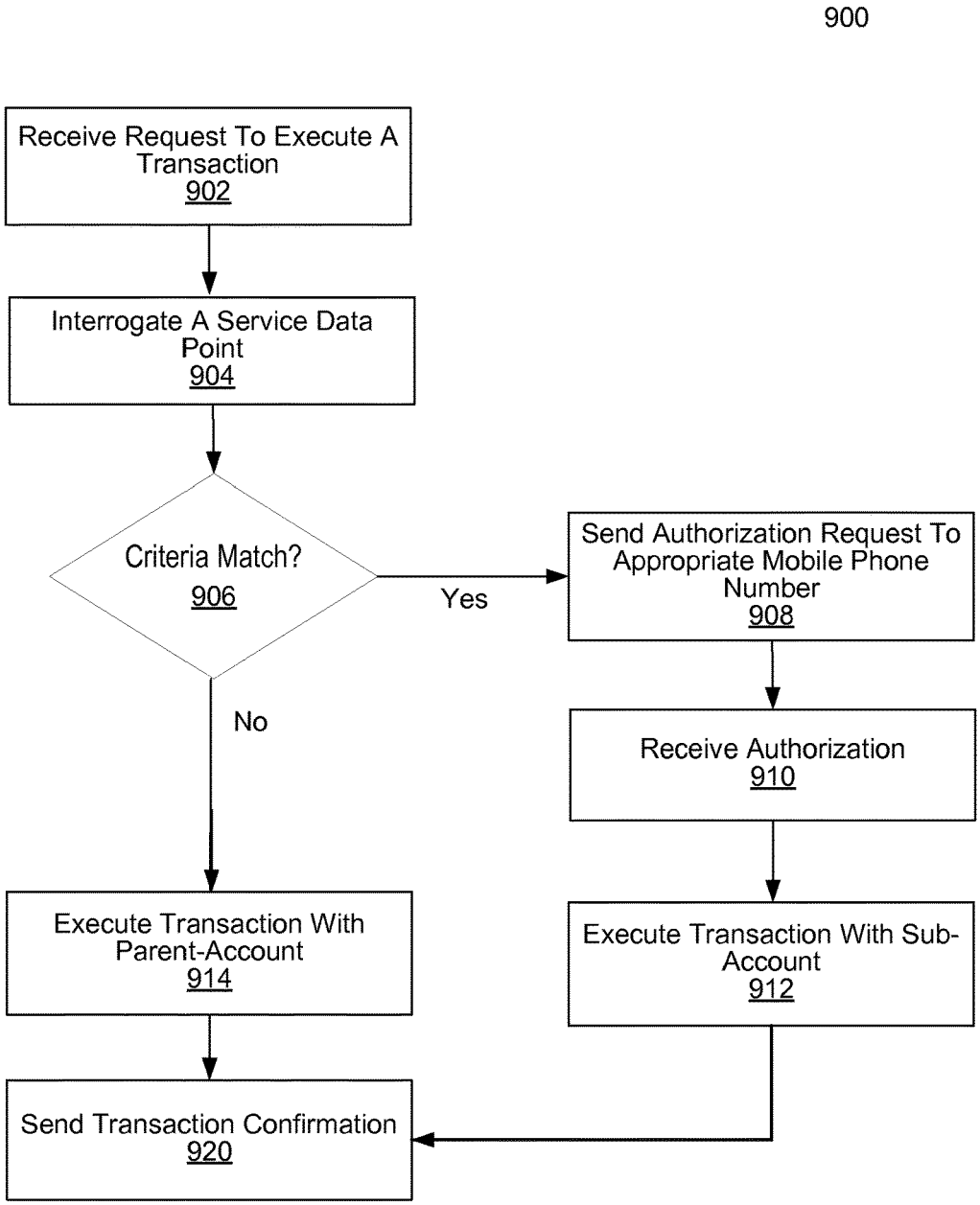

900
Receive Request To Execute A Transaction
902
Interrogate A Service Data Point
904
Criteria Match?
906
Yes
No
Send Authorization Request To Appropriate Mobile Phone Number
908
Receive Authorization
910
Execute Transaction With Sub-Account
912
Execute Transaction With Parent-Account
914
Send Transaction Confirmation
920

FIG. 9

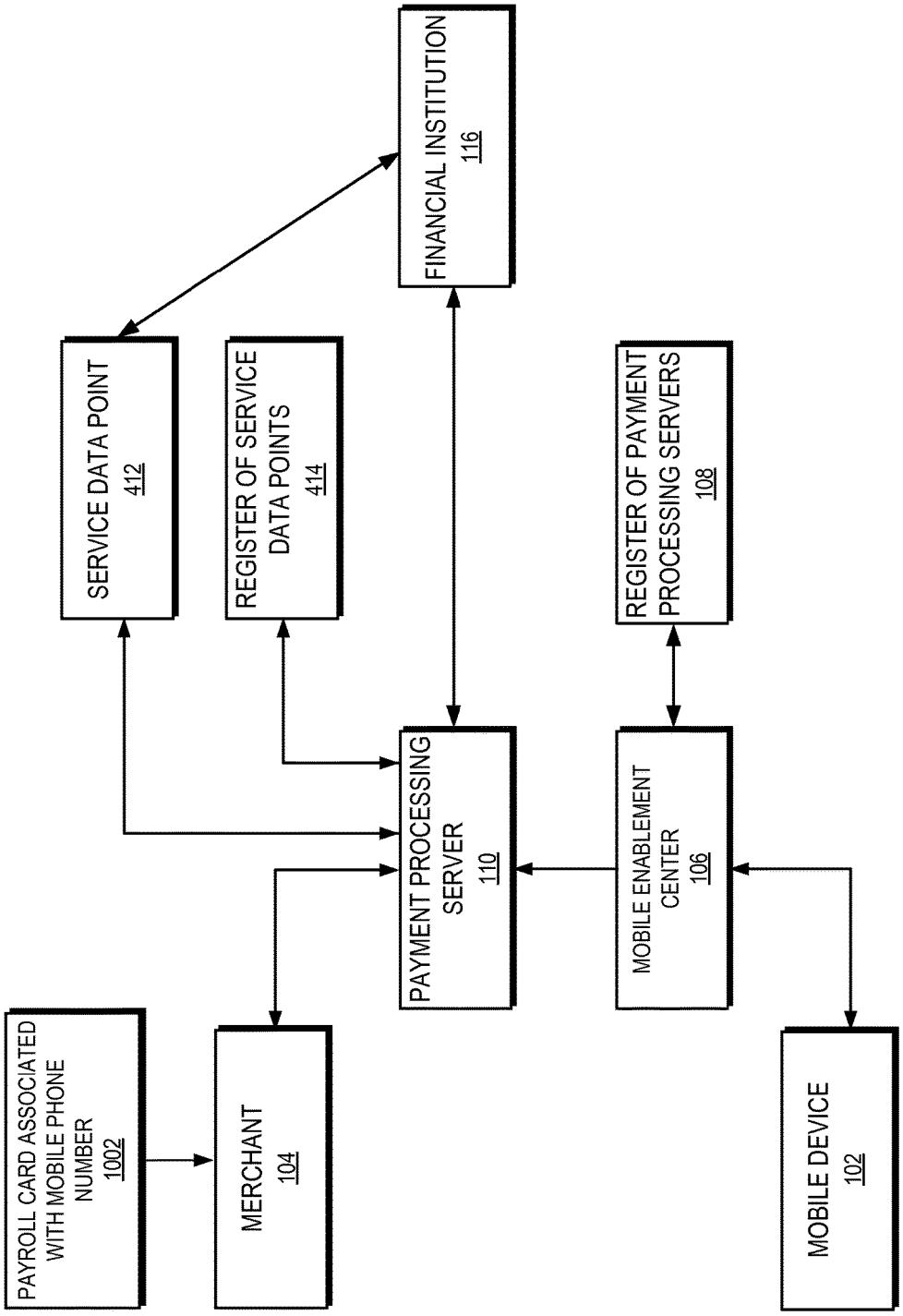

FINANCIAL INSTITUTION
116
SERVICE DATA POINT
412
REGISTER OF SERVICE DATA POINTS
414
REGISTER OF PAYMENT PROCESSING SERVERS
108
PAYMENT PROCESSING SERVER
110
MOBILE ENABLEMENT CENTER
106
PAYROLL CARD ASSOCIATED WITH MOBILE PHONE NUMBER
1002
MERCHANT
104
MOBILE DEVICE
102

FIG. 10

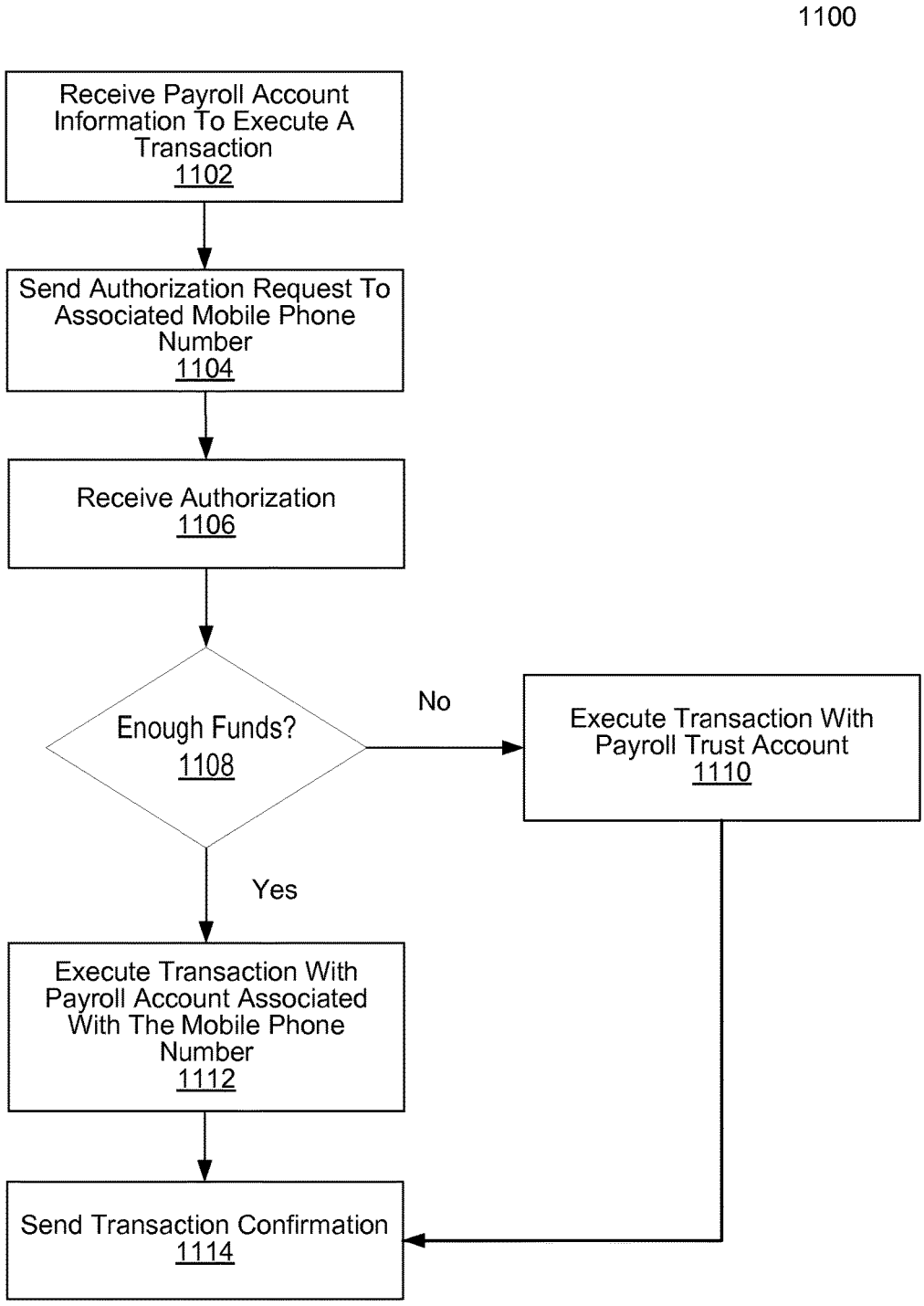

1100
Receive Payroll Account Information To Execute A Transaction
1102
Send Authorization Request To Associated Mobile Phone Number
1104
Receive Authorization
1106
Enough Funds?
1108
No
Execute Transaction With Payroll Trust Account
1110
Yes
Execute Transaction With Payroll Account Associated With The Mobile Phone Number
1112
Send Transaction Confirmation
1114

FIG. 11

MOBILE PAYMENT STATION SYSTEM AND METHOD

RELATED APPLICATIONS

This application is a continuation application of U.S. application Ser. No. 12/906,989 filed on Oct. 18, 2010, and claims priority from U.S. provisional application No. 61/279,322 filed on Oct. 19, 2009, each of which is incorporated by reference herein in its entirety.

FIELD OF THE INVENTION

This invention generally relates to the field of electronic commerce and more particularly to using mobile communication devices to execute a commercial transaction.

BACKGROUND OF THE INVENTION

Using a credit card, debit card, payroll card, senior benefit card, ATM card or any stored value card (hereafter credit card) and a point of sale terminal to purchase one or more items from a merchant has become commonplace. For example, in order to initiate a point of sale, a merchant can enter the total sale amount in a terminal. The merchant can receive a credit card from the customer to process the sale. Once the customer's credit card information is entered in a point of sale terminal, the information is sent to servers associated with a clearing house. The clearinghouse can authenticate the credit information and route the transaction based on the routing numbers associated with the credit card. The clearing house can execute a transaction with an appropriate financial institution and provide a confirmation of the executed transaction to the merchant's point of sale terminal. The merchant can print a confirmation of the executed transaction to receive a customer's approval.

Such a method of executing a transaction is beneficial because it is quick and reliable. Additionally, the customer can execute a purchase at any time regardless of whether the customer has cash on hand to purchase a product. However, such a method of executing transactions requires that the customer have a credit card. A customer can use the convenience of a card to execute transactions through a debit card if the customer has an associated debit account. However, many customers do not have bank accounts, and therefore do not have debit cards. Similarly, some customers, such as kids under a certain age may not have access to or qualify for a credit card but nevertheless may need a secure method of executing a transaction for purchase of goods.

Additionally, a customer using a credit card runs the risk of credit card fraud or fraudulent transactions. For example, if a customer's credit card is lost or stolen, another person who is not the owner of the card can execute a transaction with the card by simply presenting the card to a merchant. Since the merchant initiates the point of sale for each transaction, the clearing house and the financial institutions may not catch a fraudulent transaction unless reported by the owner of the credit card.

A customer may also not be able to use credit processing systems to execute a purchase if the customer does not have his or her card available at the merchant site. For example, a customer cannot borrow someone else's credit card to execute a transaction associated with his or her own account. Thus, credit cards or cards associated with financial institutions provide a less than optimal method for executing a transaction associated with a customer's credit or financial account.

A customer may also not be able to use credit processing systems to execute a purchase if the customer's card has a defective magnetic strip, chip or the electronic near field communication (NFC) apparatus on the card is defective. Additionally, a customer may be unable to use credit processing systems to execute a purchase if the point of sale terminal at the store is defective or has a defective NFC receiver that prevents it from reading card information.

SUMMARY OF THE INVENTION

It is a general object of the present invention to allow a customer to use a mobile communications device to initiate and execute a transaction by reversing the conventional direction of point of sale transaction initiation; that is the processing server opens communications towards point of sale terminal utilizing merchant ID or point of sale terminal ID, instead of the conventional method of point of sale terminal opening communications towards processing server.

It is a general object of the present invention to allow a customer to use a mobile communications device to initiate and execute a transaction, which overcomes the aforementioned problems with using a credit or debit card by taking advantage of the prevalence of mobile communications devices and the communications abilities of mobile devices.

It is also a general object of the present invention to allow a customer to use other methods such as calling an interactive voice response (IVR) system and using voice or dual-tone multi-frequency (DTMF) commands on a landline to initiate and execute a transaction, which overcomes the aforementioned problems with using a credit or debit card by taking advantage of the prevalence of telecommunication methods available today.

A mobile device can be used to initiate and execute a transaction with a merchant. A mobile device is used to initiate a point of sale transaction, wherein a merchant ID or, for example, a point of sale terminal ID (hereafter called "merchant ID") is sent to a payment processing server. Responsive to receiving a communication from the mobile device, the payment processing server requests transaction information from the merchant, wherein the merchant is identified based on the provided merchant ID. The merchant can provide transaction information such as the total sale amount to the payment processing server. The payment processing server can authenticate the customer and initiate a purchase transaction with the appropriate financial institutions associated with the customer and the merchant. The payment processing server can send a confirmation of the executed transaction to the merchant and the mobile device.

It is another general object of the present invention to use a point of sale terminal associated with a merchant to execute a transaction between a merchant and a customer. A merchant can provide point of sale information including the purchase amount, merchant ID and an account phone number associated with the customer. An account phone number can include a financial institution account number that belong to the customer, a phone number that is associated with a financial account number that belongs to the customer, a phone number that is used as an account number in a financial institution hereafter referred to as "account phone number.". Responsive to receiving point of sale information from the merchant, a payment processing server identifies an account associated with the account phone number and

sends an authorization request to the account phone number. The customer can enter authorization personal identification information on a communications device and send it to the payment processing server. The payment processing server can authenticate the customer and initiate a purchase transaction with the appropriate financial institutions associated with the customer and the merchant. The payment processing server can send a confirmation of the executed transaction to the merchant and the mobile device.

It is another general object of the present invention to use a payroll account associated with an account phone number to execute a transaction between a merchant and a customer. The point of sale transaction can be initiated by the merchant using the point of sale terminal or by a customer using a communications device or via an IVR call. A service data point (SDP) receives a merchant ID associated with the merchant and the account phone number associated with the customer and the payroll account. The payment processing server sends an authorization request to the account phone number. The customer can enter an authorization personal identification number on a mobile device associated with the account phone number and send it to the SDP. The SDP can authenticate the customer associated with the payroll account and initiate the purchase transaction between the merchant and the payroll account associated with the customer. The SDP can send a confirmation of the executed transaction to the merchant and the mobile device. The functionality of an SDP can be integrated in the mobile enablement center **106** and can be called either SDP or Mobile enablement center and vice versa. Similarly, the mobile enablement functionality center's functionality can be integrated in an SDP and be called the mobile enablement center or the SDP. For instance an implementation described below using an SDP can be carried out in a mobile enablement center and vice versa.

The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specification, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a high-level block diagram that illustrates a computing environment for using a mobile device to initiate a transaction according to one embodiment.

FIG. **2** is a flowchart illustrating a method of using a mobile device to initiate a transaction according to one embodiment.

FIG. **3** is a high-level block diagram illustrating a detailed view of a payment processing server for initiating a transaction using a mobile device according to one embodiment.

FIG. **4** is a high-level block diagram that illustrates a computing environment for using a mobile device to initiate a transaction according to one embodiment.

FIG. **5** is a flowchart illustrating a method of using a mobile device to execute a transaction according to one embodiment.

FIG. **6** is a high-level block diagram that illustrates a computing environment for using a mobile device to execute a transaction according to one embodiment.

FIG. **7** is a flowchart illustrating a method of using a mobile device to execute a transaction according to one embodiment.

FIG. **8** is a high-level block diagram that illustrates a computing environment for using a mobile device to execute a transaction associated with a sub-account according to one embodiment.

FIG. **9** is a flowchart illustrating a method of using a mobile device to execute a transaction associated with a sub-account according to one embodiment.

FIG. **10** is a high-level block diagram that illustrates a computing environment for using a payroll card to execute a transaction according to one embodiment.

FIG. **11** is a flowchart illustrating a method of using a payroll card to execute a transaction according to one embodiment.

The figures depict various embodiments of the present invention for purposes of illustration only. One skilled in the art will readily recognize from the following discussion that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the invention described herein.

DETAILED DESCRIPTION OF THE INVENTION

A preferred embodiment of the present invention is now described with reference to the figures where like reference numbers indicate identical or functionally similar elements. Also in the figures, the left most digit(s) of each reference number corresponds to the figure in which the reference number is first used.

Reference in the specification to "one embodiment" or to "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiments is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" or "an embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

Some portions of the detailed description that follows are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps (instructions) leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, electromagnetic, radio or optical signals capable of being stored, transferred, combined, compared and otherwise manipulated. It is convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. Furthermore, it is also convenient at times, to refer to certain arrangements of steps requiring physical manipulations or transformation of physical quantities or representations of physical quantities as modules or code devices, without loss of generality.

However, all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or

"determining" or the like, refer to the action and processes of a computer system, or similar electronic computing device (such as a specific computing machine), that manipulates and transforms data represented as physical (electronic) quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Certain aspects of the present invention include process steps and instructions described herein in the form of an algorithm. It should be noted that the process steps and instructions of the present invention could be embodied in software, firmware or hardware, and when embodied in software, could be downloaded to reside on and be operated from different platforms used by a variety of operating systems. The invention can also be in a computer program product which can be executed on a computing system.

The present invention also relates to an apparatus for performing the operations herein. This apparatus may be specially constructed for the purposes, e.g., a specific computer, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a non-transitory computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, application specific integrated circuits (ASICs), or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus. Memory can include any of the above and/or other devices that can store information/data/programs. Furthermore, the computers referred to in the specification may include a single processor or may be architectures employing multiple processor designs for increased computing capability.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems may also be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the method steps. The structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the present invention as described herein, and any references below to specific languages are provided for disclosure of enablement and best mode of the present invention.

In addition, the language used in the specification has been principally selected for readability and instructional purposes, and may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the present invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the claims.

FIG. **1** is a high-level block diagram that illustrates a computing environment for using a mobile device to initiate a transaction according to one embodiment. The computing environment may include a mobile device **102**, a mobile enablement center **106**, a register of payment processing servers **108**, a payment processing server **110**, a merchant **104** and a financial institution **116**.

FIG. **2** is a flowchart illustrating a method of using a mobile device to initiate a transaction according to one embodiment. For the purposes of discussion below, FIGS. **1** and **2** are discussed concurrently.

In one embodiment, the mobile device **102** initiates a point of sale transaction. A mobile device **102** can include any computing device having a processor and capability to communicate with others over a network or a communications link. Examples of a mobile device **102** include a cellular phone, personal device assistant (PDA), smart phone, laptop computer, desktop computer or other devices. The mobile device sends a merchant ID associated with a merchant to the payment processing server **106**. The merchant ID number is a unique identifier associated with a merchant. The merchant ID can include any information to identify or communicate with the associated number. For example, a merchant ID can include a point-of-sale terminal ID to be used by the merchant to execute the transaction. In other embodiments, the merchant ID can include an e-mail address or a phone number associated with the merchant.

In one embodiment, the customer can enter the merchant ID on to the mobile device **102** using the mobile device's input system, such as a keyboard or a touchpad etc. In other embodiments, the merchant ID information can be received by a camera on the mobile device **102**. In other embodiments, the merchant ID information can be displayed in plain view for customer to use. In other embodiments, the merchant ID information can be displayed in alphanumeric or bar code format for customer to use. In other embodiments, the merchant ID information can be received by the mobile device **102** through a communications link such as BLUETOOTH communications or RFID communications fields. For example, a merchant can have a point-of-sale terminal which broadcasts the merchant ID to mobile devices via a BLUETOOTH, laser, radio, infrared or close range electromagnetic field communications link. In one embodiment, the mobile device **102** sends the received merchant ID to another party over a communications network.

The mobile device **102** can use any available communications (COMM) method to send the merchant ID to the mobile enablement center **106**. It can use unstructured supplementary service data (USSD), short message service (SMS), multi-media message service (MMS), IVR, email, short message peer-to-peer (SMPP), Internet browser, an application executing on a mobile device, widget executing on a computing device, hard button (key), soft button (key) or any communication method available in the art in various wired or wireless technologies such as but not limited to code division multiple access (CDMA), wideband code divisional multiple access (WCDMA), integrated digital enhanced network (iDEN), Global System for Mobile Communications (GSM), one or more generations of wireless telephone technology, such as 2G, 3G, 4G, or any future generations of wireless telephone technology, Bluetooth, WiFi, worldwide interoperability for microwave access (WiMAX), Radio (short wave or other), infrared or any other communication method or protocol known in the art. Such a communication or other examples of communication are referred to herein, among other names, as COMM.

The mobile device **102** can use any available communications method (COMM) to send the merchant ID to the mobile enablement center **106**. In one embodiment, the mobile device **102** can send the merchant ID in an SMS message over a mobile communications network, such as GSM, iDEN or CDMA networks in any setup that could be 2G, 3G, 4G or any future evolution of wireless technology. In other instances, the mobile device can send multi-media messages (MMS). For example, the customer can take a picture of a barcode or a number identifier associated with the merchant ID and send the picture over a communications

network. In another instance an application executing on the mobile device **102** can interpret or recognize the barcode or number identifier associated with the merchant ID to send over a communications network. In other embodiments, the communications network used by the mobile device **102** depends on the network capabilities of the mobile device **102**. For example, the mobile device can connect to a WiFi Network and send the merchant ID via email to the payment processing server **106** over the network. In one embodiment, the customer can enter the merchant ID via IVR from a landline telephone. In other embodiments, the customer can use a user interface associated with an application executing on the mobile device **102** to send the merchant ID to the mobile enablement center **106** over a communications network. The network used to connect the mobile device **102**, the merchant **104**, the mobile enablement center **106**, the payment processing server **110**, the service data point **112** and the financial institution **116** is described in greater detail below.

In one embodiment, the merchant ID is sent to an appropriate payment processing server **110**. For example, a customer can provide a pre-set preference, wherein all transactions executed with the mobile device **102** are associated with a particular financial institution and routed through a particular payment processing server **110**. In an embodiment IPV6 protocols can be used to route the communications request to an appropriate payment processing server **110**. In another embodiment, the mobile device **102** sends the merchant ID to a mobile enablement center **106** over a communications network to be routed to an appropriate payment processing server **110**.

The mobile enablement center **106** is a platform that routes outgoing messages from the mobile devices **102** to the appropriate payment processing server **110**. The mobile enablement center **106** can receive routing requests from several service broadcast operators, such as mobile phone network operators, including GSM or CDMA network operators, landline phone operators, LAN operators, etc. For example, when mobile devices **102**, including landline or VOIP phones send an outgoing message, the service broadcast operator associated with the device or the phone number receives the outgoing message request. The service broadcast operator routes the outgoing message to the broadcast operator associated with the intended recipient of the message. In an embodiment of the invention, the mobile enablement center **106** receives a routing request from the service broadcast operator associated with the mobile device **102** or directly from the mobile device **102**. In one embodiment, the mobile enablement center **106** routes the message to an appropriate payment processing server **106** based on the outgoing message's phone number, the intended recipient's phone number, the merchant ID included in the message or any other data associated with the phone number. For example, if a user's phone number is associated with a particular financial institution **116**, the mobile enablement center **106** routes the message to a payment processing server **110** associated with the financial institution **116**.

In one embodiment, the payment processing server **110** interrogates a registry of payment processing servers **108** to identify an appropriate payment processing server **110**. For example a registry of payment processing servers **108** can include a listing of payment processing servers **110** based on the routing numbers or other identification information associated with each financial institution or based on coordinated new routing mechanism that may be mandated, devised or supervised by, for example, a standardization body, governmental body or consortium body of companies or leaders in the field.

A payment processing server **110** is a platform that executes a transaction between a customer, a financial institution **116** associated with the customer and a merchant **104**. Examples of a payment processing servers **110** include databases maintained by Visa, MasterCard, American Express, etc. In one embodiment, the payment processing server **110** receives **202** the merchant ID from the mobile device **102**. In another embodiment, the payment processing server **110** receives **202** the merchant ID in a message routed by the mobile enablement center **106**.

In one embodiment, the payment processing server **110** sends **204** a request for transaction information to the merchant **104** associated with the received merchant ID. Any communications method (COMM) known in the art can be used to communicate with the merchant **104**. For example, the payment processing center can send an SMS message, an e-mail message etc to a phone number or an email address associated with the merchant **104**. In one embodiment, the merchant ID can be associated with a merchant's unique point-of-sale terminal. In such an instance, the payment processing server **110** can send a communication to the point the particular point-of-sale terminal.

The merchant **104** can provide transaction information to send to the payment processing server **110**. Transaction information can include the total purchase price for the items the customer wants to purchase, an account number associated with the merchant, the mobile phone number provided by the customer etc. The merchant **104** can use any communications method (COMM) known in art to provide the transaction information to the payment processing server **110**. In one embodiment, the merchant can enter the total purchase amount on a point-of-sale terminal's keypad. A point of sale terminal can include a station wherein the merchant can swipe or key-in a customer's credit card or debit card to execute a purchase transaction. In another embodiment, the point of sale terminal can include a computing device, such as a machine to machine (M2M) device, mobile phone, a laptop or desktop computer, a tablet etc. In other embodiments, point of sale terminals can include established transaction terminals, such as an ATM or vending machine etc. In an instance where existing transaction terminals such as ATM or card-swipe terminals are used, the terminals can be updated via a firmware update to enable them to receive transaction information requests from a payment processing server **110**.

The payment processing server **110** receives **206** transaction information from the merchant **104**. In one embodiment, transaction information includes a phone number associated with the customer mobile device **102**. The payment processing server **110** authenticates the phone number associated with the mobile device **102**. In one embodiment, the payment processing server **110** authenticates the incoming message's phone number against the service broadcast operator network. For example, if a mobile phone number is associated with the T-MOBILE, the payment processing server **110** can query the T-MOBILE operator network **311** to identify the an account associated with the mobile phone number.

In another embodiment, the payment processing server **110** queries a register of data points **414**, described in greater detail below. Responsive to the query, the payment processing server **110** receives the account information associated with the phone number of the mobile device **102** or the

identity of the mobile enablement center **106** associated with the mobile device's **102** phone number. In one embodiment, the payment processing server **110** queries the mobile enablement center **106**. Responsive to receiving the query, the mobile enablement center **106** queries a register of payment processing server **108** to retrieve the account information associated with the mobile device's **102** phone number. Once the payment processing server **110** receives the appropriate account information, the payment processing server **110** communicates with the mobile enablement center **106** associated with the mobile device's **102** phone number and sends a transaction authorization request to the mobile device **102**. In one embodiment, the payment processing server **110** sends a transaction authorization to the merchant **102**. As described in greater detail below, upon receiving a positive transaction authorization from mobile device **102** or the merchant **104**, the payment processing server **110** initiates a transaction with an financial institution **116** associated with the account number.

As described above, the payment processing server **110** can identify an account associated with the mobile phone number **102**. In one instance, more than one account may be identified as associated with the mobile phone number. In such an embodiment, the payment processing server **110** queries a mobile enablement center **106**. The mobile enablement center **106** identifies an account associated with more than one account such as virtual accounts or real accounts that are identified as associated with the mobile phone number. In such an instance, additional logic can be used by the mobile enablement center **106** to identify an account from a list of possible accounts associated with the mobile phone number. For example, a user can provide that a debit account should be used for purchases under a certain dollar amount, such as $5. In another embodiment, the customer can associate the use of particular accounts when executing a transaction with a particular merchant. Thus, the payment processing server **110** can identify a debit account, if the merchant ID is associated with a retail merchant.

In one embodiment, the payment processing server **110** authenticates the merchant responsive to receiving the transaction information from the merchant. For example, the merchant can be authenticated if the merchant confirms the merchant ID or the customer mobile phone number initiating the transaction. In one instance, the payment processing server **110** identifies an account associated with the merchant once the authentication process is completed.

In one embodiment, the payment processing server **110** sends **208** an authorization request to the mobile device **102** that initiated the transaction request. For example, the payment processing server **110** sends a COMM, an SMS message or an email to the customer phone number or the email address initiating the transaction. In one embodiment, the payment processing server **110** can send **208** an account name and number to the mobile device **102** along with the authorization request. In another embodiment, the customer can provide a phone number associated with a customer account and a different communications phone number. For example, the customer initiating a transaction can provide an account phone number by initiating a communication from a different phone number. In such an instance, the customer can use an application executing on the communications mobile device **102** to initiate the transaction or use COMM messaging. In such an instance, the payment processing server **110** sends **208** an authorization request to the communications phone number, wherein the customer can provide an authorization associated with the account phone number. This could apply to a customer borrowing someone else's mobile device to perform his or her own transaction.

In one embodiment, the payment processing server **110** receives **210** an authorization from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **210** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

In one embodiment, the payment processing server **110** executes **212** a transaction with a financial institution. For example, the payment processing server **110** identifies a financial institution associated with the customer's account and a financial institution associated with the merchant's account, wherein the execution of the transaction comprises of debiting the purchase amount from the customer's account and crediting the purchase amount to the merchant account. In one embodiment, additional fees applied by financial institutions **116**, payment processing servers **110**, mobile enablement centers **106** can be applied to the purchase amount.

In one embodiment, the payment processing server **110** sends **214** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described below in reference to FIG. **3** can be used to send **214** the confirmations. In one embodiment, the payment processing server **110** sends the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the payment processing server **110** sends **214** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc. In another instance the payment processing server **110** sends **214** the transaction confirmation via COMM to the merchant's mobile device if one was identified by merchant as preferred delivery mechanism for confirmations

FIG. **3** is a high-level block diagram illustrating a functional view of a typical computer system **300** for use as one of the entities illustrated in the computing environment of FIG. **1** according to one embodiment. It is noted that the

computing machine **300** may also be a system or part of a system, e.g., two or more machines operating together or one or more machines operating with one or more other devices.

FIG. **3** illustrates components of a machine able to read instructions from a machine-readable medium and execute them in one or more processors and/or controllers. Specifically, FIG. **3** shows a diagrammatic representation of a machine within which mobile payment device instructions **324** (e.g., software code) can be executed to perform anyone or more of the methodologies discussed herein. In alternative embodiments, the machine operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server machine or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment.

The machine may be a server computer, a client computer, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a smartphone, a web appliance, a network router, switch or bridge, or any machine capable of executing instructions **324** (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute instructions **324** to perform anyone or more of the methodologies discussed herein.

The example computer machine **300** includes a processor **302** (e.g., a central processing unit (CPU), or group of processors, or a group of processing machines, a graphics processing unit (GPU), a digital signal processor (DSP), one or more application specific integrated circuits (ASICs), one or more radio-frequency integrated circuits (RFICs), or any combination of these), a memory **304**, including a main memory and a static memory, a network interface device **320** capable of interacting with a network **310**, an input/output device **312** (e.g., a keyboard, a cursor control device, a plasma display panel (PDP), a liquid crystal display (LCD), a projector, or a cathode ray tube (CRT)) and a storage unit **316** configured to communicate with each other via a bus.

The storage unit **316** includes a machine-readable medium **322** on which is stored mobile payment device instructions **324** (e.g., software) embodying any one or more of the methodologies or functions described herein. The mobile payment instructions **224** (e.g., software) may also reside, completely or at least partially, within the main memory **304** or within the processor **302** (e.g., within a processor's cache memory) during execution thereof by the computer system **300**, the main memory **304** and the processor **302** also constituting machine-readable media.

The external storage **317** includes a machine-readable medium on which mobile device or merchant information can be stored. In one embodiment, the machine **300** can access the external storage **317** via a communications links, as described above. In an embodiment, all components of the machine **300** can access the storage medium **317**.

While machine-readable medium **322** is shown in an example embodiment to be a single medium, the term "machine-readable medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, or associated caches and servers) able to store instructions (e.g., mobile payment device instructions **324**). The term "machine-readable medium" shall also be taken to include any medium that is capable of storing instructions (e.g., mobile payment device instructions **324**) for execution by the machine and that cause the machine to perform any one or more of the methodologies disclosed herein. The term "machine-readable medium" includes, but not be limited to, data repositories in the form of solid-state memories, optical media, and magnetic media.

The mobile payment device instructions **324** (e.g., software) may be transmitted or received over the network **310** via the network interface device **320**. In one embodiment, the network **310** is the Internet. The network **310** can also utilize dedicated or private communications links that are not necessarily part of the Internet. In one embodiment, the network **114** uses standard communications technologies and/or protocols. Thus, the network **114** can include links using technologies such as Ethernet, Wi-Fi (802.11), integrated services digital network (ISDN), digital subscriber line (DSL), asynchronous transfer mode (ATM), etc. Similarly, the networking protocols used on the network **114** can include multiprotocol label switching (MPLS), the transmission control protocol/Internet protocol (TCP/IP), the hypertext transport protocol (HTTP), the simple mail transfer protocol (SMTP), the file transfer protocol (FTP), etc. In one embodiment, at least some of the links use mobile networking technologies, including general packet radio service (GPRS), enhanced data GSM environment (EDGE), code division multiple access **2000** (CDMA2000), and/or wideband CDMA (WCDMA). The data exchanged over the network **114** can be represented using technologies and/or formats including the hypertext markup language (HTML), the extensible markup language (XML), the wireless access protocol (WAP), the short message service (SMS) etc. In addition, all or some of links can be encrypted using conventional encryption technologies such as the secure sockets layer (SSL), Secure HTTP and/or virtual private networks (VPNs). In another embodiment, the entities can use custom and/or dedicated data communications technologies instead of, or in addition to, the ones described above.

The example computer machine **300** includes a mobile network enablement unit **325** which includes the logic software (SLEE—Service Logic Execution Environment) and hardware for connecting to connect, control and communicate with any mobile network operator's node, any messaging node (such as a short message service center (SMSC), a multimedia message service center (MMSC), mail transport/transfer agent (MTA), wireless access protocol (WAP), database (DB), (session description protocol) SDP, service control point (SCP), mobile switching center (MSC), central office (CO) for wired communications, service switching point (SSP), authentication, authorization and access/accounting (AAA), gateway GPRS (general packet radio service) support node (GGSN), combined GPRS node (CGSN), packet data servicing node (PDSN), or any other node that may exists in the operator network regardless of the technology used (CDMA, WCDMA, iDEN, GSM, 2G, 3G, 4G, or future revisions of the wireless communications system, Bluetooth, WiFi, WiMax, Radio (short wave or other), infrared or any other communication method or protocol known in the art). Mobile network enablement unit **325** supports all communication protocols and standards including but not limited to instant messaging service (IMS), signaling system 7 (SS7), internet protocol (IP), transport/transmission control protocol (TCP), transaction capabilities application part (TCAP), intelligent network application protocol (INAP), mobile application part/multiple access protocol (MAP), CS1, CS2, CS3, CS4, common alerting protocol version 1 (CAP v1), CAPv2, CAPv3, CAPv4, all wireless intelligent network (WIN) standards, all intelligent network (IN) standards and all

advanced intelligent network (AIN) standards, etc. In one embodiment, the mobile network enablement unit **325** communicates with a mobile operator network **311**. As described in greater detail above, the mobile operator network **311** includes CDMA, WCDMA, iDEN, GSM, 2G, 3G, 4G, or future revisions of the wireless communications system.

Referring now to FIG. **4**, it illustrates a high-level block diagram of a computing environment for using a mobile device to initiate a transaction according to one embodiment. The computing environment may include a mobile device **102**, a mobile enablement center **106**, a register of payment processing servers **108**, a payment processing server **110**, a merchant **104**, a service data point **412**, a register of service data points **414** and a financial institution **116**.

FIG. **5** is a flowchart illustrating a method of using a mobile device to initiate a transaction using a service data point according to one embodiment. For the purposes of discussion, FIGS. **4** and **5** are discussed concurrently below.

As described in greater detail above, the mobile device **102** initiates a transaction request by sending a merchant ID to the mobile enablement center **106** or the payment processing server **110**. The payment processing server **110** receives **502** the merchant ID and sends **504** a transaction information request to the merchant associated with the merchant ID. As described above, any communications method (COMM) known in the art can be used to communicate with the merchant **104**. For example, the payment processing center can send an SMS message, an e-mail message etc to a phone number or an email address associated with the merchant **104**. In one embodiment, the merchant ID can be associated with a merchant's unique point-of-sale terminal. In such an instance, the payment processing server **110** can send a communication to the point the particular point-of-sale terminal. The payment processing server **110** can also use the commonly known ISO8583 interface to communicate with the point of sale terminal.

Service data point (also referred to as SDP) is a computing machine with, for example, all the components described above in **300**, that telecommunication operators normally use to store service logic and subscriber account balances, subscriptions, services, expiration of service dates, etc. SDPs have multiple names in different operator and vendor environments, for the purpose of this disclosure SDP refers to any and all of those nodes equivalent in function as described herein.

In one embodiment, the SDP can be used for banking, financial, investment and/or insurance operations such as keeping track of account balances, debiting accounts, crediting accounts and transferring of account funds from one account to another. A centralized SDP or SDP Register can be used to provide routing information to signals destined to a certain SDP. In an embodiment, an SDP register can be under the control, jurisdiction (auspices) of a governmental or consortium body that would regulate its functions and management.

In one embodiment the SDP communicates with financial institutions **116**, ATM machines, point of sale terminals, a mobile enablement center **106** and/or a merchant **104** for the purpose of processing point of sale transactions with financial institutions or payment processing servers **110**. For example SDP will support any standard data communication protocol and data security standards such as, but not limited to, International Standards Organization (ISO) 8583, simple object access protocol (SOAP)/extensible markup language (XML), SOAP, hypertext transfer protocol (HTTP), secure sockets layer (SSL), etc.

In one embodiment, the payment processing server **110** identifies **504** a service data point (SDP) responsive to a phone number provided by the mobile device **102**. The phone number is a customer phone number associated with the customer's banking account that is controlled by SDP. A service data point **412** is a database where customer phone numbers are stored in addition to customer account information, and where the customer's account information can be retrieved based on its associated with the provided phone number. In one embodiment, the service data point **412** can be used to control financial institution accounts.

In one embodiment, the payment processing server cannot identify an appropriate SDP based on the provided account phone number. In such an instance, the payment processing system sends an interrogation request to the registry of SDPs **414** to identify **504** an SDP associated with the customer's account phone number. The registry of SDPs **414** provides the routing information to an SDP **412** associated with the customer's banking account.

Once an appropriate SDP **412** is identified, the payment processing server interrogates the SDP to receive **506** account information associated with the customer's phone number. The SDP **412** can retrieve account information associated with the customer's phone number.

As described above, the payment processing server **110** sends **508** a transaction information request to the merchant indentified by the merchant ID. Responsive to the request, the merchant can send transaction information to the payment processing server. In one embodiment, the payment processing server receives **510** the transaction information from the merchant via communications means known in the arts. As described above, the transaction information can include the total purchase price for the items the customer wants to purchase, an account number associated with the merchant, the mobile phone number provided by the customer etc. The merchant **104** can use any communications method (COMM) known in art to provide the transaction information to the payment processing server **110**. In one embodiment, the merchant can enter the total purchase amount on a point-of-sale terminal's keypad.

As described above, in one embodiment, the payment processing server **110** sends **512** an authorization request to the mobile device **102** that initiated the transaction request. For example, the payment processing server **110** sends a COMM, an SMS message or an email to the customer phone number or the email address initiating the transaction. In one embodiment, the payment processing server **110** can send **512** an account name and number to the mobile device **102** along with the authorization request. In another embodiment, the customer can provide a phone number associated with a customer account and a different communications phone number. For example, the customer initiating a transaction can provide an account phone number by initiating a communication from a different phone number. In such an instance, the customer can use an application executing on the communications mobile device **102** to initiate the transaction, or do it using COMM messaging. In such an instance, the payment processing server **110** sends **512** an authorization request to the communications phone number, wherein the customer can provide an authorization associated with the account phone number.

In one embodiment, the payment processing server **110** receives **514** an authorization message from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for

purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **514** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (or a one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

Once a correct authorization code e.g., a PIN is received from the mobile device **102**, the payment processing server executes the requested transaction with the SDP **412**. The SDP **412** updates the account information associated with the customer. The payment processing server **110** sends a transaction confirmation to the mobile device **102** and the merchant **104**. As described above, in one embodiment, the payment processing server **110** sends **518** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described above can be used to send **518** the confirmations. In one embodiment, the payment processing server **110** sends **518** the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the payment processing server **110** sends **518** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc.

FIG. **6**, illustrates a high-level block diagram of a computing environment for using a mobile device to execute a transaction according to one embodiment. The computing environment may include a mobile device **102**, a payment processing server **110**, a merchant **104** and a financial institution **116**.

FIG. **7** is a flowchart illustrating a method of using a mobile device to initiate a transaction using a service data point according to one embodiment. For the purposes of discussion, FIGS. **6** and **7** are discussed concurrently below.

In one embodiment of the system and method described below, the point of sale is initiated by the merchant. In one embodiment, a point of sale terminal associated with the merchant **104** is used to enter and send point of sale information such as a transaction amount, a communications phone number and an account phone number. An account phone number is a phone number associated with a financial institution. For example, the customer can preset that a particular phone number is associated with a particular account with a financial institution. The account can be a credit account, a debit account, a savings account, a payroll account, etc. A communications phone number can be the phone number associated with the customer. In another instance, the communications phone number is different from an account phone number, allowing a customer to use a borrowed phone to execute a transaction. For example, if a customer realizes that he or she lost or forgot his or her mobile phone, the customer can borrow someone else's phone by requesting that a communication be sent to the phone number associated with the borrowed phone. In other embodiments, the customer can provide a communications email address or an account email address wherein, the email account is associated with a financial institution's account for the customer.

In one embodiment, the payment processing server **110** receives **702** the point of sale information from the merchant **104**. The payment processing server **110** sends **704** an authorization request to the communications phone number provided by the merchant **104**. As described above, in one embodiment, the payment processing server **110** sends **704** an authorization request to the communications phone number or the account phone number as provided by the customer. In one embodiment, the payment processing server **110** sends a COMM, an SMS message or an email to the phone number or the email address initiating the transaction. In one embodiment, the payment processing server **110** can send **704** an account name and number to the mobile device **102** along with the authorization request. For example, if the customer has associated several credit or debit accounts with an account phone number, the payment processing server **110** can provide a listing of all the accounts available to the customer. In such an instance the payment processing server **110** opens a data session to the mobile device **102** and provides a menu to choose from wherein the customer can choose the account to execute the transaction with. In another embodiment, the payment processing server **110** uses a USSD menu option if available in the network or a WAP push message with several links denoting various accounts, or communicate to a client on the mobile device **102**. Also, in such an instance, the customer can enter an authorization PIN for an account the customer wishes to use to execute the purchase. In another embodiment, the payment processing system requests one PIN even if the customer has associated several accounts with the account phone number. In such an instance, the customer can enter the authorization PIN for the account the customer wants to use to execute the purchase. The payment processing server **110** can identify a credit or a debit account based on whether the authorization PIN matches one of accounts associated with the account phone number.

In one embodiment, the customer can enter and send a message to the payment processing server **110** to authorize the transaction. The payment processing server **110** receives **706** the authorization from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated with the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, a one-time password (or a one time use PIN which expires on first use) or PIN can be used by a customer when using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant. In one

embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **706** the authorization PIN from the customer through a communications network.

Responsive to the customer sending the authorization, the payment processing server **110** receives **706** the authorization from the mobile device **102**. As described in greater detail above, the payment processing server executes **708** the point of sale transaction with financial institutions associated with the customer and the merchant **104**. Once the transaction is executed **708**, the payment processing server sends a confirmation to the merchant **104**, the communication and the account phone number associated with the customer. As described above, in one embodiment, the payment processing server **110** sends **710** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described above can be used to send **710** the confirmations. In one embodiment, the payment processing server **110** sends **710** the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the payment processing server **110** sends **710** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc.

Referring now to FIG. **8**, it illustrates a high-level block diagram of a computing environment for using a mobile device to execute a transaction associated with a sub-account according to one embodiment. The computing environment may include a mobile device **102**, an SDP **412**, an account associated with the mobile phone number **810** and a sub-account associated with the mobile phone number **812**.

FIG. **9** is a flowchart illustrating a method of using a mobile device to execute a transaction associated with a sub-account according to one embodiment. For the purposes of discussion, FIGS. **8** and **9** are discussed concurrently below.

As described in greater detail above, the mobile device **102** or the merchant **104** can initiate a transaction request by sending a merchant ID and an account phone number to a service data point (SDP) **412**. In one embodiment, the SDP receives **902** the transaction request either from the merchant **104** or from the mobile device **102**. In one embodiment, the SDP is interrogated **904** to determine if the received account phone number is associated with a sub-account. A sub-account **812** is associated with the a parent account **810** wherein the sub-account may have limited access to the funds available to the parent account **810** or the account associated with the mobile phone number. If the SDP determines that the account phone number is associated with a sub-account, the SDP provides that a sub-account criteria is matched **906**.

In other embodiments, the sub-account criteria can be matched **906** in other ways. For example, a phone number can be associated with a sub-account. In such an instance, if a communications phone number matches the sub-account **812** criteria, the SDP executes **912** a transaction with the sub-account responsive to receiving the appropriate authorization. In other embodiments, an authorization PIN can be associated with a sub-account. If the sub-account criteria are met, the SDP sends an authorization request to one or more of the communications phone number, a phone number associated with the sub-account or a phone number associated with the parent account **810**. For example, the SDP or the payment processing server **110** can send **908** an authorization request to the account phone number associated with the parent account **810** or the phone number associated with the sub-account, or both. As such, a customer can create a sub-account for a family member, such that the customer's children or other family members can make certain purchases using their own mobile device. Similarly, in an embodiment wherein the authorization request is sent to a phone number associated with the parent account **810**, the parent can provide real-time approval or rejection of certain purchases initiated by the sub-account holder.

As described above, in one embodiment, the payment processing server **110** sends **908** an authorization request to an appropriate mobile device **102** including the mobile device **102** that initiated the transaction request or to a phone number associated with the parent account **810**. For example, the payment processing server **110** sends an SMS message or an email the phone numbers or the email address provided. In one embodiment, the payment processing server **110** can send **908** an account name and number to the appropriate mobile device **102** along with the authorization request. In another embodiment, the customer can provide a phone number associated with a customer account and a different communications phone number. For example, the customer initiating a transaction can provide an account phone number by initiating a communication from a different phone number. In such an instance, the customer can use an application executing on the communications mobile device **102** to initiate the transaction or use COMM messaging. In such an instance, the payment processing server **110** sends **908** an authorization request to the communications phone number, wherein the customer can provide an authorization associated with the account phone number.

The SDP can receive **910** the authorization from the sub-account phone number, the communications phone number or the phone number associated with the parent account **810**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the payment processing server **110** receives **910** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (or a one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is different than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

The SDP can initiate an execution of the transaction between the customer and the merchant **104**. If the SDP does not receive an appropriate authorization or a sub-account criteria match, the SDP executes **914** the transaction with the parent-account **810**. As described in greater detail above, a transaction confirmation is sent to the merchant, the communications phone number, the account phone number or the sub-account phone number.

FIG. **10** is a high-level block diagram that illustrates a computing environment for using a payroll card to execute a transaction according to one embodiment. The computing environment may include a mobile device **102**, a mobile enablement center **106**, a register of payment processing servers **108**, a payment processing server **110**, a merchant **104**, a service data point **112**, a register of service data points **114** and a financial institution **116**.

In one embodiment the SDP could control an aggregate account (also referred to as a Nostro Account) in a bank that includes multiple sub accounts that can represent payroll accounts. Such payroll accounts could be used for those that cannot establish an account on their own because of lack of sufficient funds or lack of good credit. Such aggregate accounts could be accessed by any payment processing server **110** or SDP if they are associated with a mobile phone number. One such subaccount in an aggregate account can have multiple virtual accounts. For example a worker with no bank account would ask employer to use such subaccount for direct deposit of payroll. The subaccount would be associated with the workers mobile phone number. The worker would be able to create multiple virtual sub-subaccounts on the SDP and move funds to those sub-subaccounts. Each sub-subaccount would be associated with a mobile phone and could be accessed by phone with the aid of any payment processing server **110** or mobile enablement center **106**. In one embodiment the SDP can take the place or perform the functions of the mobile enablement center. In one embodiment the SDP can control fund transfer between banks, phone account numbers and between merchants.

FIG. **11** is a flowchart illustrating a method of using a payroll card to execute a transaction according to one embodiment. For the purposes of discussion, FIGS. **10** and **11** are discussed concurrently below.

In the embodiment discussed in reference to FIGS. **10** and **11**, the point of sale transaction is initiated by a merchant **104** or a mobile device **102**, wherein the account phone number is associated with a payroll card **1002**. A payroll card **1002** can be a debit card associated with a payroll account. An employer of the customer using the payroll card can deposit payroll checks in the payroll account. For example, instead of giving the customer a weekly, bi-weekly or monthly payroll check which can be either cashed or deposited, the employer can make weekly, bi-weekly or monthly payroll deposits to the payroll account, such that the employer would not have to issue new payroll checks each payroll cycle. Such a system is beneficial because it reduces the employer's cost of issuing checks. Additionally such a system is beneficial to employees because they have access to an account associated with a card which can be used to make purchases without opening additional accounts or a new line of credit with another financial institution. Additionally, each payroll account can be associated with a payroll trust account. A payroll trust account is an aggregate of accounts used by the employer to make deposits to each individual payroll account associated with an employee. The payroll trust account generally carries a float and cannot be closed. As described in greater detail below, an additional benefit of the system and method described herein is to allow customers to borrow funds from the trust account if the funds in the their customer payroll accounts are depleted. The payroll trust account can withhold money due to the employee in the next payroll period. The withheld money can be a portion of the borrowed money, the entirety of the borrowed money or the entirety of the borrowed money in addition to fees and interests.

In one embodiment, the payment processing server receives **1102** a request to execute a transaction from an account associated with the payroll card **1002**. For example, a merchant can swipe or enter the account number associated with the payroll card on a point of sale terminal. In such an instance, the point of sale terminal can receive a firmware update to enable a customer to use a payroll account card to execute a purchase. In another embodiment, a mobile device can be used to initiate a point of sale transaction. As described above, the mobile device can send an account phone number and a merchant identification to a service data point (SDP) **412** or to a mobile enablement center **106**. In another embodiment, as described above, the customer can borrow a mobile computing device to initiate a point of sale transaction.

Upon receiving the request, the SDP sends **1104** and receives **1106** appropriate authorization information to a mobile phone number associated with the payroll account or communications phone number. As described above, in one embodiment, the SDP **412** sends **1104** an authorization request to the mobile device **102** associated with the payroll account. For example, the SDP **412** sends an COMM, SMS message or an email to the customer phone number or the email address associated with the payroll account. In one embodiment, the SDP **412** can send **1104** an account name and number to the mobile device **102** along with the authorization request. In another embodiment, the payment processing server can send **1104** authorization request to communications phone number different from the account phone number associated with the payroll account. For example, a communications phone number can be provided in the communication received **1102** providing payroll account information to execute a transaction. In such an instance, the customer can use an application executing on a mobile device **102** associated with the communications phone number to initiate the transaction.

In one embodiment, the SDP **412** receives **1106** an authorization from a mobile device **102**. The authorization message can include a personal identification number (PIN) associated the customer's account. A customer can set multiple PINs for one or more accounts. For example, the customer can set a PIN for purchases under a preset dollar amount and a different PIN for purchases over a dollar amount. Similarly, the customer can set a separate PIN for particular merchants. In another embodiment, the customer can have a distinct PIN (or a one time use PIN which expires on first use) when the communications phone number initiating the transaction is different from the phone number associated with the customer. In one embodiment, the mobile device **102** associated with the communications phone number is configured to delete all instances of the PIN from the mobile devices' on-board or off-board memory. In such instances, the SDP **412** receives **1106** the authorization PIN from the customer through a communications network. In another embodiment, a one-time password (or a one time use PIN which expires on first use) can be used by a customer using a communications phone number different than the account phone number. For example, a customer can preset a one-time password (that expires on first use) for instances when the communications phone number is dif-

ferent than the account phone number, for purchases over a certain dollar value or for purchases with a particular merchant.

An SDP logic identifies whether the payroll account has enough funds **1108** to execute the requested transaction. If so, the SDP executes **1112** the transaction with a bank associated with the payroll card. If the SDP determines that the payroll account does not have sufficient funds, the SDP executes **1110** a transaction with the payroll trust account. Once the transaction is complete, a transaction confirmation is send to the merchant and the mobile device associated with the payroll account. In one embodiment, the SDP **412** sends **1114** a transaction confirmation to the mobile device **102** and the merchant **104**. Any communications method (COMM), such as an SMS message, an email address, a phone call or described above can be used to send **1114** the confirmations. In one embodiment, the SDP **412** sends **1114** the confirmation to a point-of-sale terminal associated with the merchant ID. In such an instance, the point-of-sale terminal can print a copy of the confirmation for the merchant's or the customer's records. In an instance wherein the communications phone number is different than a phone number associated with the transaction account, the SDP **412** sends **1114** a transaction confirmation to one or both phone numbers. The confirmation communication can include details about whether the transaction was successfully completed, the date and time of the confirmation, the total transaction amount etc.

While particular embodiments and applications of the present invention have been illustrated and described herein, it is to be understood that the invention is not limited to the precise construction and components disclosed herein and that various modifications, changes, and variations may be made in the arrangement, operation, and details of the methods and apparatuses of the present invention without departing from the spirit and scope of the invention as it is defined in the appended claims.

What is claimed is:

1. A method for conducting a transaction between a terminal and a customer by a payment processing server, the customer using a mobile device, the method comprising:

receiving, at the payment processing server, a terminal identifier from the mobile device operated by the customer, the terminal identifier indicating a request to initiate a transaction with a terminal identified by the terminal identifier, wherein the terminal identifier does not indicate a transaction amount for the transaction;

sending, at the payment processing server, in response to receiving the terminal identifier, a transaction information request to the terminal associated with the terminal identifier;

receiving, at the payment processing server, transaction information from the terminal in response to the transaction information request, the transaction information including the transaction amount for the transaction;

identifying, at the payment processing server, a customer account associated with the customer and a terminal account associated with the terminal; and

initiating, at the payment processing server, the transaction between the customer account and the terminal account for the transaction amount received from the terminal.

2. The method of claim **1**, wherein the terminal is an automated teller machine (ATM).

3. The method of claim **1**, wherein the customer account is a payroll account.

4. The method of claim **1**, wherein the customer account is identified based on a telephone number associated with the mobile device.

5. The method of claim **1**, wherein the customer account is identified based on an email address associated with the mobile device.

6. The method of claim **1**, wherein the identified customer account is one of a plurality of sub-accounts associated with a parent account.

7. The method of claim **1**, further comprising requesting an authorization from a second mobile device prior to initiating the transaction between the customer account and the terminal account.

8. The method of claim **1**, further comprising requesting an authorization from the mobile device, wherein the authorization comprises receiving a personal identification number (PIN) or password from the mobile device and determining that the PIN or password matches an authorization PIN or password.

9. The method of claim **8**, wherein the authorization PIN is a one-time PIN.

10. The method of claim **8**, wherein the authorization PIN varies based on the transaction amount.

11. The method of claim **8**, wherein the authorization PIN varies based on the terminal.

12. The method of claim **8**, wherein the identified payment account is selected from a group of payment accounts associated with the customer, and the authorization PIN varies based on the selected payment account.

13. The method of claim **1**, wherein the terminal identifier is received by the mobile device by user entry on the mobile device, identified from a scanned code by the mobile device, or received by the mobile device using near field communication (NFC).

14. The method of claim **1**, wherein the mobile device is located remotely from the terminal.

15. The method of claim **1**, wherein the terminal identifier is at least one of a landline number, a phone number, or an email address.

16. A non-transitory computer-readable medium for conducting a transaction between a terminal and a customer, the customer using a mobile device, the medium comprising instructions for execution by a processor on a payment processing system, the instructions, when executed by the processor causing the processor to perform the steps of:

receiving a terminal identifier from the mobile device operated by the customer, the terminal identifier indicating a request to initiate a transaction with a terminal identified by the terminal identifier, wherein the terminal identifier does not indicate a transaction amount for the transaction;

sending, in response to receiving the terminal identifier, a transaction information request to the terminal associated with the terminal identifier;

receiving transaction information from the terminal in response to the transaction information request, the transaction information including the transaction amount for the transaction;

identifying a customer account associated with the customer and a terminal account associated with the terminal; and

initiating the transaction between the customer account and the terminal account for the transaction amount received from the terminal.

17. The non-transitory computer-readable medium of claim **16**, wherein the terminal is an automated teller machine (ATM).

18. The non-transitory computer-readable medium of claim **16**, wherein the customer account is a payroll account.

19. The non-transitory computer-readable medium of claim **16**, wherein the customer account is identified based on a telephone number associated with the mobile device.

20. The non-transitory computer-readable medium of claim **16**, wherein the customer account is identified based on an email address associated with the mobile device.

21. The non-transitory computer-readable medium of claim **16**, wherein the customer account is one of a plurality of sub-accounts associated with a parent account.

22. The non-transitory computer-readable medium of claim **16**, wherein the instructions further cause the processor to perform the step of requesting an authorization from a second mobile device prior to initiating the transaction between the customer account and the terminal account.

23. The non-transitory computer-readable medium of claim **16**, wherein the instructions further cause the processor to perform the step of requesting an authorization from the mobile device, wherein the authorization comprises receiving a personal identification number (PIN) or password from the mobile device and determining that the PIN or password matches an authorization PIN or password.

24. The non-transitory computer-readable medium of claim **23**, wherein the authorization PIN is a one-time PIN.

25. The non-transitory computer-readable medium of claim **23**, wherein the authorization PIN varies based on the transaction amount.

26. The non-transitory computer-readable medium of claim **23**, wherein the authorization PIN varies based on the terminal.

27. The non-transitory computer-readable medium of claim **23**, wherein the identified payment account is selected from a group of payment accounts associated with the customer, and the authorization PIN varies based on the selected payment account.

28. The computer-readable medium of claim **16**, wherein the terminal identifier is received by the mobile device by user entry on the mobile device, identified from a scanned code by the mobile device, or received by the mobile device using near field communication (NFC).

29. The computer-readable medium of claim **16**, wherein the mobile device is located remotely from the terminal.

30. The method of claim **16**, wherein the terminal identifier is at least one of a landline number, a phone number, or an email address.

* * * * *

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MOBILE EQUITY CORP.

(b) County of Residence of First Listed Plaintiff Collin
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

William E. Davis III
213 N. Fredonia St., Ste 230

DEFENDANTS

WALMART INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☒ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☒ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	☐ 880 Defend Trade Secrets Act of 2016	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	SOCIAL SECURITY	☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 861 HIA (1395ff)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
				☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS		☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	**Habeas Corpus:**	IMMIGRATION		☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 462 Naturalization Application	FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence	☐ 465 Other Immigration Actions	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General		☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			☐ 950 Constitutionality of State Statutes
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	**Other:** ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement			
	☐ 448 Education				

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
35 U.S.C. §281 et seq

Brief description of cause:
Infringement of U.S. Patent Nos 8,589,236 and 10,535,058

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*

JUDGE _____ DOCKET NUMBER _____

DATE
4/7/2021

SIGNATURE OF ATTORNEY OF RECORD
William E Davis III

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.